TXT29-1-1® Power Service Guide

Version 2021.01.27

Information to Insight

www.intrado.com/Life-Safety

Contents

Intrado

1. Introduction

This service guide describes Intrado's TXT29-1-1 Power service (the "Service"). Service is a solution offering emergency delivery of SMS to the short code 911 over an Internet Protocol ("IP") network. Emergency text messages, initiated from all Carriers requested by the PSAP within the PSAP jurisdiction, are routed to the public safety agency ("Customer") using text initiator cell sector location and displayed on the Power 911® screen at the call taker positions. Thereafter call takers may engage in a text dialogue with the caller to establish the nature of the emergency and dispatch accordingly.

Supporting Service is Internet Transport Services ("ITS") or Intrado's A9-1-1® Routing service for Text delivery to Customer. ITS provides managed edge devices and a secure VPN over Customer provided Internet between the PSAP and the Intrado Data Center to support Service. Similarly, the Intrado A9-1-1 Routing service can be used to establish equivalent connectivity.

2. Service Overview

2.1. Description

Service enables Customer's call taker ("End-User") to receive and respond to an emergency service request using an SMS text message. Service provides a messaging gateway, routing services, and a communications interface for emergency service requests sent via SMS text message to 9-1-1.

Intrado's Text Control Center ("TCC") is able to simultaneously process, route, and track emergency text dialogues for multiple Service customers. On receipt of a new SMS message a session is established between the TCC and Power 911 workstation with a visual indication on the workstation that there is a new text message. An available End-User selects the TEXT button to answer the request and to send and receive text messages with the text initiator ("TI"), referred to as a text dialogue.

2.2. Service Features

Service includes the following features:

- Visual alert to End-User that an emergency text message has arrived
- Ability to accept, complete, and place in queue any incoming text messages
- Pre-loaded and configurable messages to make responses quick and efficient
- End-User may respond to a text message while on a voice call, if they so choose
- Ability to display TI location as an in band message
- Ability to automatically failover to a back-up PSAP if connectivity to the primary PSAP is lost or text equipment at the PSAP fails
- Log retention of text dialogues
- Back-up/Failover
- External Transfer
- Location Update
- MMS Delivery
- Configurable Timeout Timer

2.2.1. Internal Transfer

TCC now supports a variety of "in-band" commands that can be sent by the PSAP to invoke certain feature-specific actions on the TCC. Transfer is initiated utilizing the #T command.

- Allows 2 PSAPs to correspond privately utilizing the #P command
- Conference in another PSAP
- Transfer text dialog to another PSAP
- Upon a PSAP transfer the LAST known location is forwarded, in the initial message.
- Airbus Vesta CPE PSAPs utilize their own transfer ability and not this in-band TCC command. Their internal transfer ability is developed within their own software.

2.2.2. External Transfer

External PSAP transfer extends the existing transfer function utilizing the same #T command to prompt a transfer.

- External PSAP transfer allows for transfer of TXT29-1-1 dialogs to PSAPs using a different TXT29-1-1 TCC provider, other than Intrado.
- In order to utilize the external transfer function the PSAP must be Intrado text enabled.
- The PSAP receiving the transfer does not need to be Intrado text enabled.
- External transfer operates like the internal Intrado PSAP transfer functionality.
- Upon text enablement with Intrado, key words will be established for selected PSAPs to support transfer.
- Upon text enablement with Intrado, settings can be configured to allow for multiple transfers of a text dialog, allowing for an unlimited amount. The default setting for multiple transfers is 10.

2.2.3. Back-up/Failover

Back-up/Failover allows for a PSAP to designate an alternate PSAP to receive its TXT29-1-1 messages if the PSAP does not answer a text within 30 seconds. This is an optional service.

- Designation of a primary and secondary PSAP
- Messages continue to try the primary
- Route to secondary after 30 seconds if no answer (this is a universal setting, non-configurable)

2.2.4. Location Update

TCC allows the special command, called the “locate command”, to obtain updated location information of an emergency texter. Specific keywords provide the PSAP call taker with the ability to request a location update for an active dialog.

- #L is the command used by the PSAP call taker.
- Upon a PSAP transfer, the LAST known location is forwarded in the initial message.

2.2.5. Media Delivery Configurable by Carrier & PSAP

Media and media notifications are available to PSAPs that opt-in for receipt. The PSAP will opt-in or out at the time of requesting service. A project is underway to address the PSAPs that are already text enabled that want to establish MMS delivery in the below outlined method.

How it works:

- PSAPs pre-configure three email addresses where TCC will auto-send media files. This removes the need for PSAPs to call Intrado to retrieve their media files.
- PSAPs can have the ability to choose whether they would like to receive MMS files or not. The default, upon deployment, is set to not send MMS. If the PSAP chooses to shut MMS off after opting in, they need to put in a ticket with the help desk for Mobility Sys Admin.
- If the PSAP call taker does not have immediate access to the pre-configured mailbox(es) receiving the media files, an in-band command can be initiated to have the media sent immediately to an email of its designation ex. #email Janedoe@psap.com. The PSAP policy will dictate if the call takers utilize this command.
- A PSAP will be able to transfer media files to another PSAP. Example- If PSAP A initiates a transfer to PSAP B as long as PSAP B elects to receive media, the files are transferred. If PSAP B has opted out of receiving media files, they will remain logged at PSAP A.
- Group MMS messaging is not available. Example: The texting party is having a heart attack and text messages 9-1-1 and their spouse. The message will go through to 9-1-1. It is the responsibility of texting application provided by the carrier to manage this situation, NOT TCC.
- MMS size limitations are based on what the carrier can accept. The default is set to 5MB which is the largest carrier requirement encountered to date. If this increases in the future, we can scale to the increased limits required by the carrier.

- If a carrier does not deliver MMS to a PSAPs jurisdiction that PSAP cannot accept MMS from that carrier.
- MMS plain text is delivered to the PSAP in its original state uninterrupted. If non-text MMS media is received and the PSAP is not prepared or has not opted in to receive MMS, the non-text media is not sent to the PSAP and a message is sent to the texting party informing them that the image, video, audio, etc. was not delivered to the PSAP.

2.2.6. Configurable Timeout Timer

The TCC has a configurable timer that will terminate the text dialog after a period of inactivity. The default time value is 120 minutes. The timer can be applied on a per PSAP basis. When the activity timer triggers, the TCC sends a canned message to the texter informing them that the session has timed-out.

2.2.7. Customer Program Support

Customer designates operations contact to act as Customer's project lead for this agreement. Customer's project lead works with the Intrado program manager to:

- Assist with the coordination of Intrado and Customer technical resources
- Coordinate Customer's technical resources for planning and design and requirements definition
- Reporting and verify problems related to Service
- Facilitate ongoing communications with Intrado
- Assign appropriate Information Technology ("IT") Personnel and experienced End-Users at each PSAP who understand the overall impact of the transition of the 9-1-1 systems
- Customer to provide ongoing resource for end-to-end testing of Service

Note: This activity may include Intrado and Customer's appropriate technical and operational groups to assure a solid understanding of the network architecture, data exchange procedures, PSAP needs, standard operational procedures, and services as designed for Customer.

Intrado will provide 24 hour per day operational support for Service. Intrado will provide appropriate contact information to Customer. Intrado is dependent on Customer to provide timely and accurate information to resolve problems.

Customer will identify personnel and work with Intrado to schedule training.

2.2.8. Daily Operational Support and Escalation Procedures

Intrado will provide daily operational support to the extent outlined in the service order for Customer. Intrado will provide appropriate contact information to Customer. Intrado is dependent on Customer or Customer's PSAP to provide timely and accurate information to resolve problems. Failure of providing timely and accurate information to Intrado will impair the ability to resolve escalated incidents.

2.2.9. Subpoena Compliance

Intrado will reasonably comply with requests made by Customer for specific subpoena-related audit record data. Intrado can accommodate most requests within five business days, provided that the request contains the full call back number (Wireless Text call), PSAP name, and a specific date and time. Requests for data that are vague or require extensive research will not be processed until additional detail is provided by Customer.

Requests that require extensive research will be subject to additional charge.

2.2.10. System Audit Records

Intrado will store system audit logs for the Intrado systems involved in 9-1-1 text processing. For example:

- Text service transcripts

Intrado stores system audit logs for minimum one year. Intrado can provide pricing for data recovery past the service order term, on request.

2.3. Data Transport

2.3.1. A9-1-1 Routing Service for Text Delivery

Customers utilizing Intrado's A9-1-1 Routing Service can leverage their existing transport to facilitate Service delivery to the PSAP. The point of demarcation for Customer A9-1-1 service connectivity is the same as described in the diagrams provided below.

2.4. ITS Overview

ITS monitors Service over managed edge devices and a secure VPN through a Customer provided Internet connection between Customer and the Intrado Data Center.

ITS routers are deployed in either single-router or dual-router architecture. Each ITS router is dual-homed to geographically-redundant POPs within the Intrado ESInet. All application connectivity will traverse a device with border-control functionality ("BCF") to reach elements within the Intrado ESInet such as the TCC for delivery of Intrado's Integrated Service as shown in Figure 1.

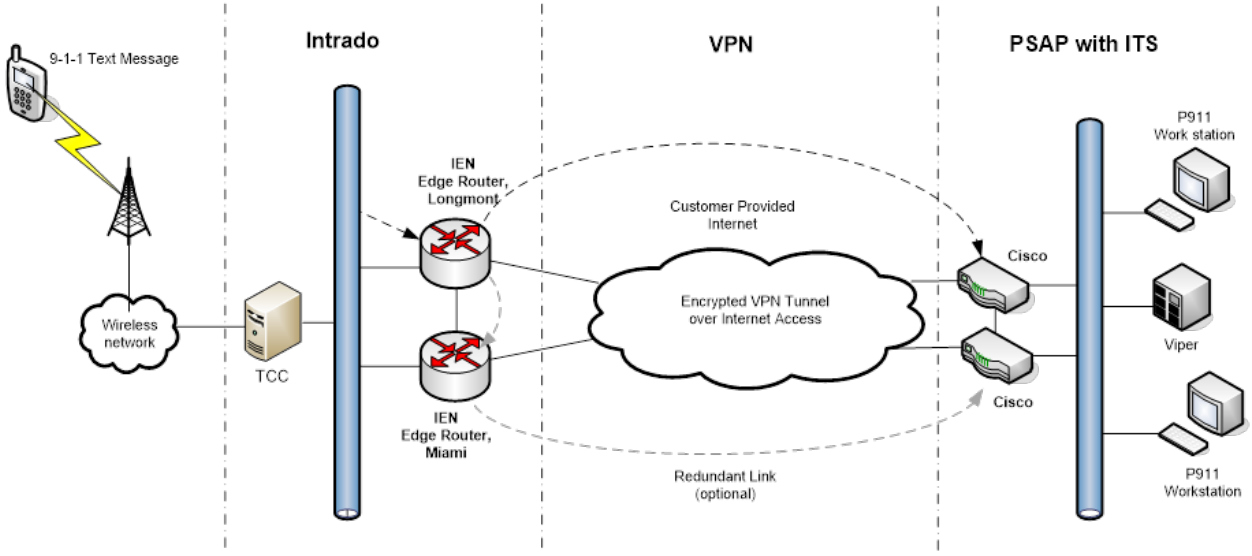

Figure 1: TXT29-1-1: High Level Diagram

ITS is deployed in one of three configurations:

a. Host-Remote/Multi-node/ESInet
b. Standalone PSAP with shared use public IP connection (non-Isolated)
c. Standalone PSAP with dedicated public IP connection (Isolated)

2.4.1. Service Use Cases

The only supported use case for ITS is the Intrado Service.

2.4.2. Host-Remote/Multi-node/ESInet Requirements

The Host-Remote/Multi-node/ESInet architecture is suited for PSAPs or host sites which are part of larger deployments (host/remote, multi-node, etc.). Use this option when ITS routers will be deployed at multiple sites within Customer's PSAP network/ESInet and dynamic cross-site failover is required. This design requires Customer to purchase routers/firewalls if they do not have them already (they should have them if they are running a host/remote or multi-node setup). This option also meets i3 best practices (assuming Customer-managed router/firewall serves as a BCF device).

In this design, routing between ITS routers and Customer-managed routers/firewalls is dynamic (to support cross-site failover).

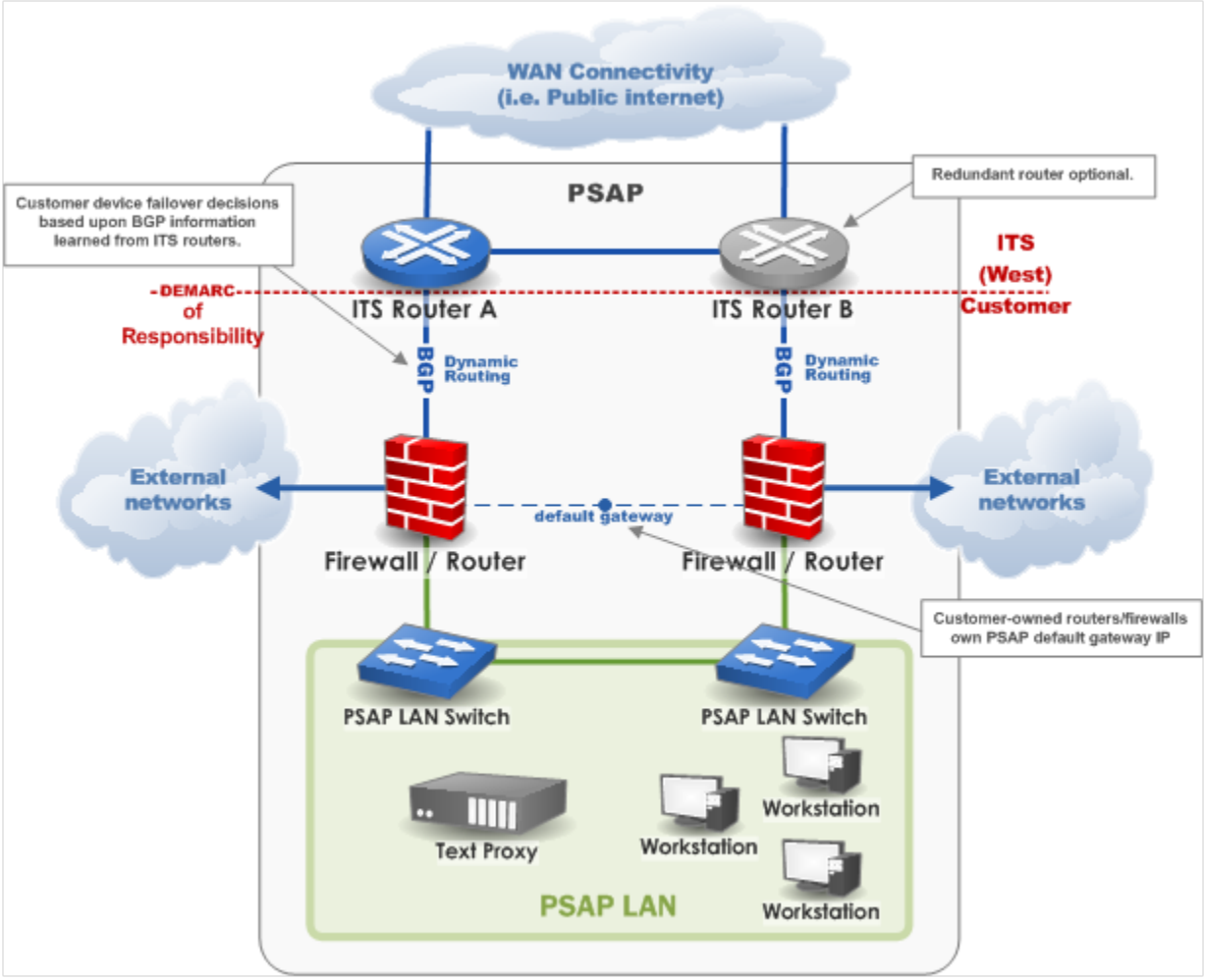

Figure 2: Host-Remote/Multi-node/ESInet Architecture

2.4.2.1. Host-Remote/Multi-node/ESInet PSAP Requirements

- Site is part of a host/remote or multi-node deployment.
- Customer must maintain routers & firewalls to interconnect with ITS routers.
- Customer router/firewalls must support the BGP routing protocol.
- Customer router/firewalls must have one free port per ITS router.
- Uplinks to ITS routers must be Ethernet patch cables.
- Uplinks to ITS routers must be set to 100Mb/full-duplex.

2.4.3. Standalone non-Isolated PSAP

The standalone non-isolated PSAP architecture is suited for simple standalone PSAPs that currently have or will require connectivity to other (non-Intrado) networks. In this design, ITS routers connect to Customer-managed routers or firewalls to reach the PSAP LAN. This option also meets i3 best practices (assuming Customer-managed router/firewall serves as a BCF device). This design requires that Customer purchase routers/firewalls if they do not have them already (they should have them if they are routing to external networks).

In this design, routing between ITS routers and Customer-managed routers/firewalls is static.

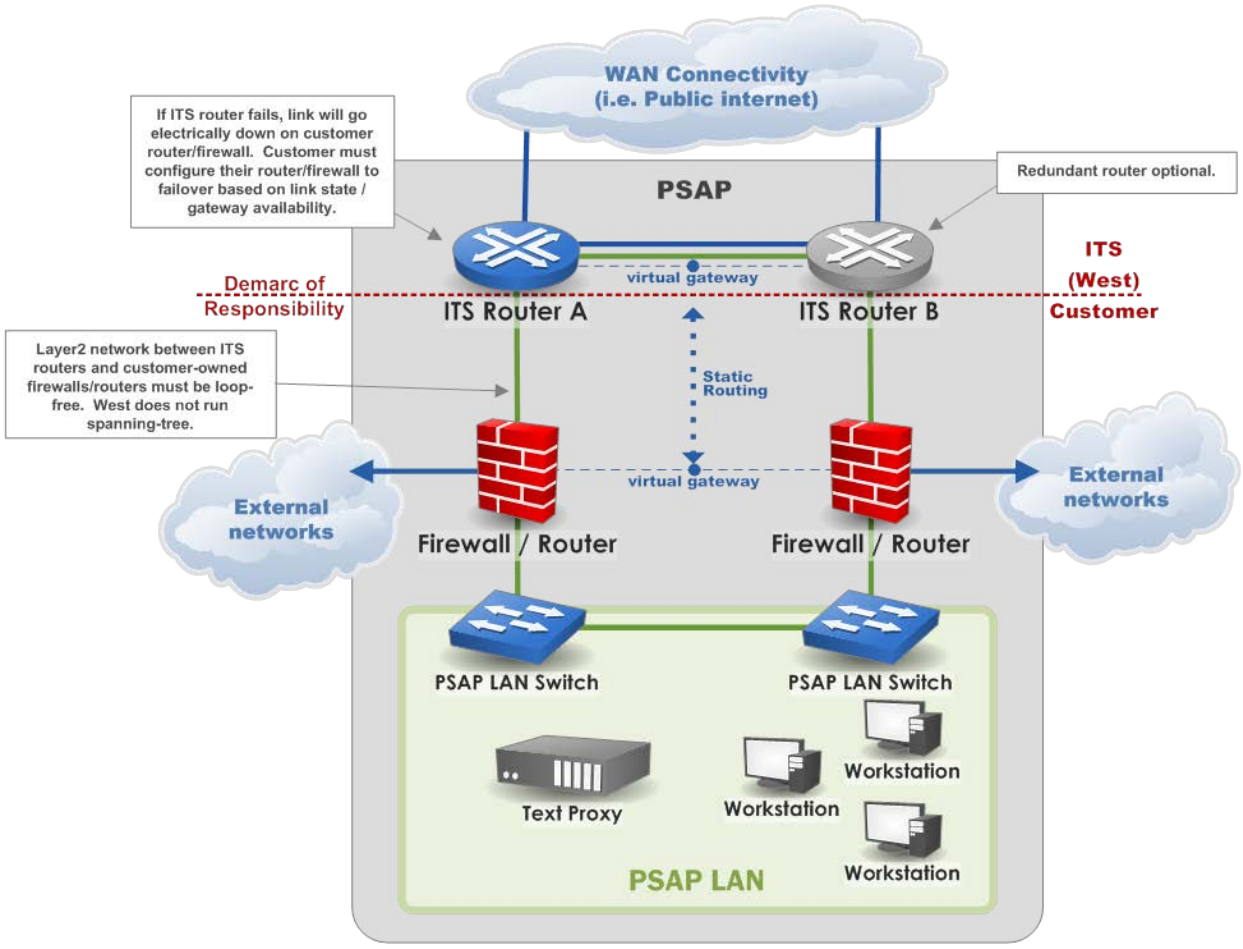

Figure 3: Standalone non-Isolated PSAP ITS Architecture

2.4.3.1. Standalone non-Isolated PSAP Requirements

- PSAP is not part of a host/remote or multi-node deployment.
- Customer must maintain routers & firewalls to interconnect with ITS routers.
- If Customer routers/firewalls are redundant, they must be clustered/stacked, or use a first-hop reachability protocol such as HSRP/VRRP.
- Customer router/firewalls must have one free port per ITS router.
- Uplinks to ITS routers must be Ethernet patch cables.
- Uplinks to ITS routers must be set to 100Mb/full-duplex.

2.4.4. Standalone Isolated PSAP

In a standalone isolated PSAP configuration, the ITS router takes over the PSAP LAN gateway, which makes this option the fastest and least complex to implement. However, it requires that the existing PSAP LAN has no routing whatsoever to external networks. This option does not use a BCF between Customer network and ITS routers. If Customer requirements call for a BCF, either the standalone non-isolated PSAP or the Host-Remote/Multi-node/ESInet architecture solution must be provided.

Figure 4 illustrates the LAN connectivity model for standalone PSAPs that do not have external network connectivity.

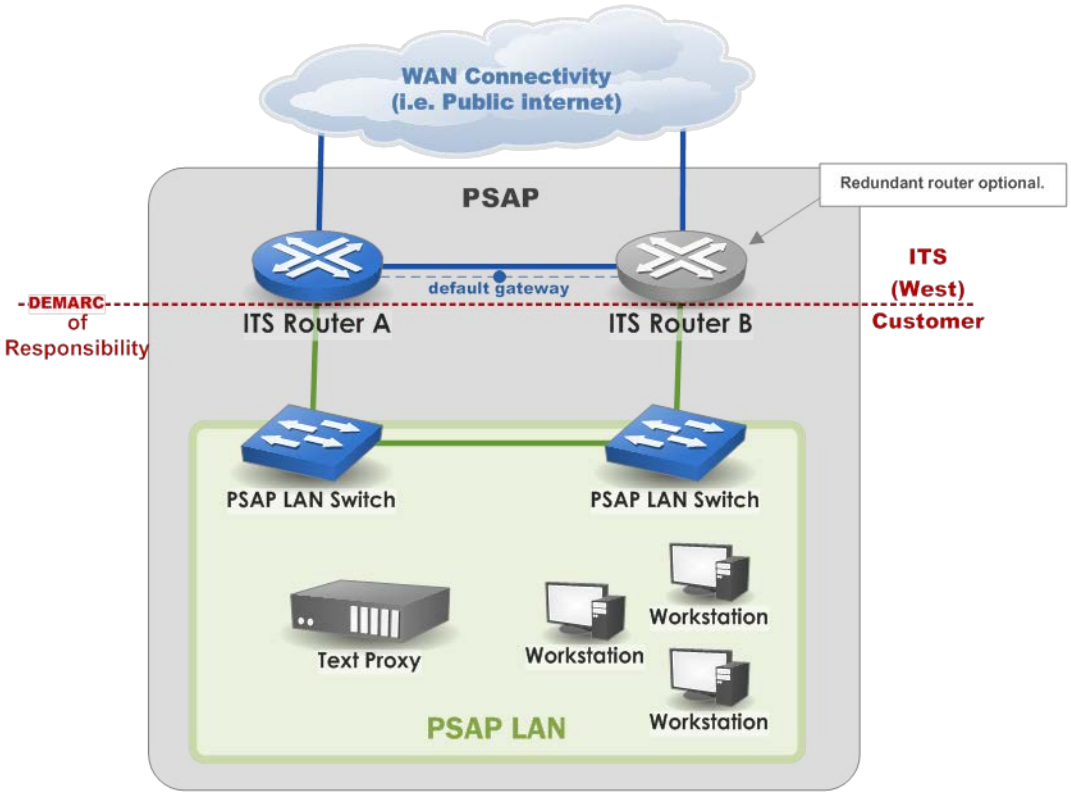

Figure 4: Standalone Isolated PSAP ITS Architecture

2.4.4.1. Standalone Isolated PSAP Requirements

- PSAP must be completely isolated from other IP networks, and is not part of a host/remote or multi-node deployment.
- ITS routers will take over the PSAP LAN default gateway IP.
- PSAP LAN switches must have one free port per ITS router.
- Uplinks to ITS routers must be Ethernet crossover cables.
- Uplinks to ITS routers must be set to 100Mb/full-duplex.

2.5. Customer Provided Public Internet

Customer provided public Internet access is required for establishment of VPN transport from the Intrado Data Center to the PSAP. The public Internet bandwidth will be dependent upon the agreements established by the PSAP and its Internet Service Provider ("ISP"). Intrado cannot make any guarantees on bandwidth for this transport path. Given a heartbeat of 1 check per minute, 3 Mbps of bandwidth will be consumed as an ITS baseline with expected bursts of 8192 Bps for the text application.

The following are the requirements and method of handoff to facilitate proper connectivity between the Intrado ESInet and ITS routers co-located at Customer:

Customer must provide internet connectivity via an Ethernet handoff to the ITS router. This link must be hard-set for 100Mb/full-duplex. If the handoff is from a router, the Ethernet cable must be a cross-over cable.

Customer must provide ITS router with an IP via DHCP (preferred), or by static assignment. If static, Customer must provide an IP, subnet mask, and gateway.

Each ITS router requires a separate internet connection.

Internet connections should be plugged into GE 0/1 port on the ITS router.

Communication between the ITS routers and the following IP addresses/ports/protocols must be permitted.

IP addresses	Ports/Protocols
64.58.49.24	ICMP
64.58.49.25	UDP 500
64.58.49.26	UDP 4500
64.58.51.56	IP Protocol 50
64.58.51.57	

Customer is responsible for managing its ISP(s), and all infrastructure up to (but not including) the ITS router port.

2.6. TXT29-1-1 Failover Protection

Failover protection for TXT29-1-1 is provided for solutions that purchase a second (redundant) ITS. With a redundant ITS there are two forms of failover support for Service-ITS failover (network layer), TXT29-1-1 alternate routing (application layer).

Network Layer Failover: For standalone non-isolated PSAPs, ITS failover is accomplished via link state/gateway availability failure detection by the ITS' firewall/router. For host-remote/multi-node/ESInet architectures failover is accomplished via BGP routing. In both cases failover is accomplished in the matter of a few seconds.

Application Layer Failover: In cases where the routing to the primary PSAP TXT29-1-1 Serving Area User Agent ("SAUA") has failed, the TXT29-1-1 TCC can be configured to route to an alternate SAUA. The alternate SAUA must be a separate physical facility and have its own primary NENA PSAP ID (FCC 9-1-1 Master Registry). This failover capability only exists for host-remote/multi-node/ESInet solutions where the primary and secondary PSAPs each has its own primary PSAP NENA IDs. This failover occurs 30 seconds after the Intrado TCC fails to connect to the primary SAUA. Establishment of the alternate SAUA is associated with the provision of Service.

3. Severity Levels

Intrado will address all service issues, whether identified by Intrado or by Customer, according to the Intrado-confirmed Severity Level. Severity Levels determine the appropriate contact procedure and the actions that will be taken by Intrado for initial notification time, status update time, and incident management.

Following are service disruption definitions and procedures for each Severity Level and the response time goals for each Severity Level:

3.1. Severity Level 1

Severity Level 1 is only covers Voice and ALI delivery. It does not apply Service.

3.2. Severity Level 2

Intrado systems supporting Service are completely inoperative or severely impacted, resulting in complete loss in delivery of Service.

Resolution Procedure: Intrado will apply immediate and sustained effort until a resolution is in place. If a resolution cannot be readily identified, Intrado will initiate internal escalation procedures to assure resources are appropriately assigned for problem resolution efforts. Systems supporting Service are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.

3.3. Severity Level 3

Intrado systems supporting Service are impaired, where major functions are operative but functioning at limited capacity or critical elements are no longer redundant.

Resolution Procedure: Intrado will correct Service disruption or provide a procedure for the PSAP to bypass or work around such disruption in order to continue operations if possible. If a bypass procedure is utilized, Intrado will provide PSAP with an action plan for the development of the final resolution, and Intrado will continue resolution activity until full service is restored to PSAP.

3.4. Severity Level 4

Intrado systems supporting Service are impaired and some functions are not operating, but those functions are not mandatory or critical to 9-1-1 text delivery or are considered minor or cosmetic and have only a minor impact on usability.

Resolution Procedure: Intrado will address via standard maintenance procedures during Intrado normal business hours. If a software fix is required, Intrado will provide a fix during the next scheduled software release.

3.5. Onsite Response Time Goals

The on-site response time goals are stated in the chart below. On-site response times will apply if Intrado determines it is necessary to go on-site to repair a problem with Service.

Severity Level	On-Site Response Time Goal
1	Not Applicable
2	12 hours

4. Responsibility Matrix

The following matrix outlines the typical responsibilities of each party for the implementation and ongoing provision of Service. Where both parties have been listed, additional detail on the responsibilities of each party is included in the sections below. Failure of a party to satisfactorily complete a required task could materially impair Intrado's ability to provide Service.

Task	Responsibility
Project Implementation	
Project Management	Intrado/Customer
Develop Intrado Methods and Procedures	Intrado
PSAP Facilities	Customer
PSAP Facility Site Preparation (floor space, power, etc.)	Customer
PSAP Data Collection	Customer
Text Routing Cell Sector Data	Intrado
Non-Intrado PSAP Equipment Note: This may be legacy equipment or new equipment purchased under another Customer agreement and or non-Intrado PSAP equipment, such as CAD system, voice recording equipment, and radio system; if applicable	Customer
End to End Testing of Service Prior to Production	Intrado/Customer

Task	Responsibility
Production Turn-up of Service	Intrado/Customer
Ongoing Responsibilities	
TCC Log Storage and Backups	Intrado
TCC Network Maintenance	Intrado
TCC Network Monitoring	Intrado
ITS Network and System Maintenance	Intrado
Data Transport	Intrado/Customer
Public Internet Service Maintenance (where applicable)	Customer
Text Application Upgrades	Intrado
Text Log Storage and Backups	Intrado
Maintain Intrado Methods and Procedures	Intrado
Problem Reporting, Triage and Resolution	Intrado/Customer

Table 1: Responsibility Matrix

4.1. Intrado Responsibilities

Intrado will provide and maintain geographically redundant TCC systems.

Intrado will interconnect with Wireless Carrier SMS hubs to route SMS generated by the participating Wireless Carrier subscribers to Customer. Only 9-1-1 text traffic originating from the participating Wireless Carrier subscribers will be routed to Customer.

Intrado will monitor and alarm the Intrado Network to proactively detect any hardware application failures.

Intrado will perform monitoring of communications between the VIPER® and the Intrado Network.

When Intrado detects a service affecting event, or upon request by Customer, Intrado will perform troubleshooting for issues that are within the direct control of Intrado for IP connectivity to the SMS hub provider. Intrado will contact the SMS hub provider, as necessary, for support issues related to SMS hub network.

4.2. Customer Responsibilities

Customer will provide personnel to participate and help execute the end-to-end system acceptance test plan. Customer participation includes providing call takers to receive and process test text messages at pre-scheduled timeframes.

Customer will ensure that the workstations have been upgraded to current versions of software supporting the required VIPER and Power functionality.

Customer will provide Internet access conforming to minimum requirements as specified in Section 2.5 above.

Customer will provide rack space for the Intrado communications equipment (routers/switches and remote power/console servers) in Customer's equipment room within 100 feet of the communications demarcation point. The Intrado communications equipment requires one rack unit slot per router and will come with brackets to support installation in a standard 19-inch equipment rack. Customer will ensure the equipment rack that houses the Intrado communications equipment is adequately grounded and anchored (to the floor, ceiling or adjacent racks). Customer will also provide commercially reasonable physical security for Intrado provided communications equipment. Intrado recommends that Customer-provided rack space be in a

location that receives limited building traffic. Customer will also provide an AC power feed (110v/1.5A) for the Intrado communication equipment.

Note: This activity may include coordination between Intrado and Customer's appropriate technical and operational groups to assure a solid understanding of the network architecture, data exchange procedures, PSAP needs, standard operational procedures, and services as designed for Customer.

Customer will not impair or prevent Intrado's ability to provide Service. If such occurs and is not remedied within 90 days of Intrado's request to proceed and with all parties acting in good faith, then Customer will be obligated to compensate Intrado for services rendered and/or for cost incurred to put the infrastructure in place to attempt to render Service.

5. Service Limitations and Disclaimers

The following service limitations and disclaimers apply:

- Service cannot be enabled until Customer has modified its network to route to the Intrado TCC.
- PSAP billing will begin upon completion of deployment and text readiness delivery from Intrado to the PSAP. Completion is defined as the PSAP being able to accept text messages.
- Intrado interconnects with third party TCC's, however the performance of the third party TCC is not the responsibility of Intrado.
- Intrado's responsibility for text message routing and processing begins when text messages have been delivered to the Intrado TCC and is limited to the routing and delivery of text messages from Intrado to the identified Customer's End-User. Intrado is not responsible for the delivery or timing of SMS Request for Assistance text messages through the carrier networks.
- Network failures could result in Service being temporarily unavailable. Due to the SMS network and/or wireless carrier servers, new and in-process text dialogues could be delayed or lost.
- End-User cannot initiate a text session with a caller.
- TXT29-1-1 interface will not bid the ALI system nor receive an ALI response for text messages. No ALI-like data will be provided for text messages.
- Service is an emerging technology and is not a replacement for established landline and wireless 9-1-1 services. Service relies on industry SMS infrastructure which is not built to public safety standards, and may include increased latency and the potential for dropped messages.
- Service requires that mobile phones must be text-enabled and be capable of sending properly formatted text messages.
- Intrado has no control over the truncating and sequence delivery of SMS messages.
- Intrado has no control over the character count limitations per device and/or carrier network.
- Intrado has no control or authority to mandate the content of bounce back messages.
- Intrado has no control of routing messages that do not come to the Intrado TCC.
- Intrado has no control over improper routing of SMS messages from third party TCC providers.
- Intrado Outage Notification is limited to Intrado systems and will not include carrier network specific information.
- ITS is not an option to support voice 9-1-1 calls or ALI services.
- Intrado's responsibility for service performance is limited to its equipment and Intrado-provided network.
- Customer understands and accepts that the overall service availability of Customer-provided Internet path will be impacted by the reliability of the Internet connection provided by Customer. Customer takes sole responsibility to restore the Internet connection with its selected ISP.
- Equipment charges will be assessed upon delivery of equipment.
- Solutions where the TXT29-1-1 solution requires transport to remote PSAPs will require use of Customer WAN solution connecting the PSAPs. Unless provided by Intrado, Customer understands and accepts that the overall service availability impacted by outages on Customer WAN. Unless provided by Intrado, Customer takes sole responsibility to restore the Internet connectivity between its geographically dispersed locations.
- After installation of ITS circuit, Customer has three days to acknowledge acceptance of Service or acceptance will be assumed and monthly billing for the ITS will commence.

- A transfer initiated must be initiated from a PSAP using the Intrado TCC. However the transfer can be destined for a non-Intrado TCC PSAP.
- Transfers delivery may be limited to the primary PSAP designated within a circle shape file. The shape file is determined by the PSAPs TCC provider.
- Airbus Vesta CPE PSAPs can use the external transfer capability.
- Backup/Failover is an optional feature.
- Backup/Failover feature will allow auto failover to the designated secondary PSAP after 30 seconds of the text not being answered at the primary PSAP.
- Intrado is limited to providing updated location information based on what is provided from the carriers commercial location servers.
- Intrado is not responsible for the delivery of MMS to the TCC.
- Intrado will only email the MMS to the pre-configured email addresses provided by the PSAP.
- MMS will only be delivered to a PSAP that requests MMS delivery.