Medtel Communications
4732 E State Road 64 | Bradenton, FL 34208
941-751-7780 | 941-933-1133 | www.medtelcom.com

Fax

TO:	Toby L Welch	FROM:	Medtel Communications
FAX:	304-558-3970	PAGES:	76
PHONE:		DATE:	08/14/2023
RE:	CRFP AGO2400000001	CC:	

☐ Urgent ☐ For review ☐ Please comment ☐ Please reply ☐ Please recycle

VENDOR NAME: Medtel Communications LLC
BUYER: Toby L Welch
SOLICITATION NO.: CRFP AGO2400000001
BID OPENING DATE: *TECHNICAL OPENING* - Thursday August 10,2023
BID OPENING TIME: 1:30 p.m.
FAX NUMBER: 304-558-3970

Medtel Communications

Department of Administration
Purchasing Division 2019 Washington Street East
Charleston, WV 25305-0130

VENDOR NAME: MEDTEL COMMUNICATIONS
BUYER: Toby L Welch
SOLICITATION NO.: CRFP AGO2400000001
BID OPENING DATE: *TECHNICAL OPENING* - Thursday August 10,2023
BID OPENING TIME: 1:30 p.m.
FAX NUMBER: 304-558-3970

Cloud-Based Telephony System
Presented by Medtel Communications

Medtel Communications Cover Page	p. 1
Medtel Communications Response Letter	p. 2
About Medtel Communications	p. 3
Medtel Communications Info Sheet	p. 4
Product Line-Up and Supported Services	p. 5
Bid Response Questions	p. 6-14
4.3.1 Qualification and Experience	p. 15
4.4 and 4.5	p. 16
Medtel Reliability and Redundancy	p. 17
Enterprise-Grade Security	p. 18
Medtel Communications Customer Examples	p. 19
4.2.2.1 Security - Attachment A	p. 20-21
4.2.2.1 Security Architecture – Attachment B	p. 22-25
4.2.2.1 Data Protection Policy & Procedures – Attachment C	p. 26-52
4.2.2.6 Vendor References Medtel Communications – Attachment D	p. 53
Medtel Communications – Disaster Recovery & Business Continuity Attachment E	p. 54
Medtel Communications – Service Level Agreement – Attachment F	p. 55-62
State of West Virginia Centralized Request for Proposals Info Technology (authorized signature)	p. 63
Designated Contact Form (authorized signature)	p. 64
ADDENDUM ACKNOWLEDGEMENT FORM SOLICITATION NO.:CRFP AGO24*001 (authorized signature)	p. 65
6.8 Availability of Information	p. 66
8 Commercial General Liability Insurance Cyber Liability Insurance	p. 67
Medtel Yealink T54W Phone Brochure	p. 68-69
Medtel Yealink WH63 DECT Wireless Headset brochure	p. 70-71
Medtel T5 Series Quick Reference Guide	p. 72-75

Medtel™
Communications

To: State of West Virginia

August 8, 2023

Fr: Bryan Webb
Medtel Communications
President & CEO

Subject: RFP Submission for Statewide Telephony System

Medtel Communications recognizes this is an incredible opportunity to not only be the RIGHT solution for the State of West Virginia's telephone system but the most SCALABLE in the industry. As you will see from our RFP submission, a few things will stand out versus others that you look at in this process:

1. Technical Perspective - Medtel's product will meet the needs of the State of West Virginia. The system is completely scalable supporting the initial rollout for first 200 phones in the Attorney General's Office; as well as the expansion across the State to the nearly 10,000 additional users.

2. Customer Support – Medtel's support for our customers is second to none in the industry. Currently, when a customer needs support, there is no multi-step Interactive Voice Response System that takes a customer 20 minutes to receive help. We have more of a 'white glove' support system where phones are answered by a live person (in the United States) on a 24/7 basis. Depending on the severity of the issue, the call is routed to the right support team for quick resolution.

3. Product Innovation – At Medtel, we pride ourselves on continuously evaluating our products, determining what our customers need and ensuring our products evolve to meet the needs of our customers. Our company has been built on a solid base of customers that continues to grow every day. The State has our commitment that we will continue to provide a product that meets your needs today and will continue to evolve in the future.

4. Training – Medtel is dedicated to ensuring your users are properly trained on the telephony systems functions to ensure they are productive and getting the maximum benefit from the system. Depending on the audience, these can be a mix of 'On-site, In-Person' Training to Online Webinars and Short Videos if that proves to be more efficient for your employees. Medtel is committed to your success on this project.

5. Financial Value – As you will see in the proposal, the price is extremely competitive if not below that of the competition. However, we differentiate ourselves with the Quality of our Product, our Product Innovation, Live Person Support, and our Training. We are giving a significant discount on all the equipment needed by the State of West Virginia as well as keeping our monthly pricing and training at very competitive levels.

If you have any questions about the RFP, please don't hesitate to ask us for clarification.
I am confident you will see that Medtel Communications is the RIGHT partner for ALL THE RIGHT REASONS, not just a price comparison. We look forward to serving your employees in the future.

Regards,
Bryan Webb
President & CEO

Medtel™ Communications

About Medtel Communications

Medtel Communications is an innovator in the telecommunications industry, providing cloud-based unified communications, contact center, and collaboration tools for businesses nationwide. Medtel is built upon a 50-year history of telecommunications innovation and experience. The company began with the design and manufacturing of traditional PBX phone systems, leading to the development of an enterprise-class proprietary cloud communications platform.

Medtel is committed to helping businesses adapt to ever-changing workplace demands for communication and collaboration by providing extremely reliable, easy to use, stable products and software applications. Medtel Communications delivers successful communication solutions to organizations in the private, public, and government sectors.

Medtel's M-Cloud Solution is scalable and can meet the demands of the State of West Virginia's requirements based on user count and call volume.

Additionally, Medtel's M-Cloud Platform offers the following benefits:

- All in one platform with voice, chat, audio, and video conferencing
- VoIP Business Phone Service with 40+ advanced features
- Real-time call analytics and reporting for actionable insights
- Easy setup and configuration with admin and user portals
- Geo-redundant network for secure, reliable service

Our teams of engineers, developers, and support personnel are highly skilled in implementing and supporting telecommunications and cloud solutions. More importantly, they are dedicated to the delivery of quality products and services.

Full legal name of the company: Medtel Communications LLC

Year business was established: 2013

Medtel™ Communications

All the Features You Need on One Platform

Medtel's business phone system combines phone service, messaging, presence, chat, and conferencing on a single cloud-based platform. Whether you require desk phones, softphones (PC) or smartphone apps, our suite of products and services are configured to suit the needs of your business.

Our Solutions

Business Phone System

Contact Center

Audio & Video Conferencing

Microsoft Teams Integration

Work from Anywhere

Make and receive work calls from your desk phone, mobile device, computer, or tablet.

Why Medtel?

- All in one platform with voice, chat, audio and video conferencing
- VoIP Business Phone Service with 40+ advanced features
- Simple, all-inclusive pricing for predictable, low monthly cost
- Real-time call analytics and reporting for actionable insights
- Easy setup and configuration with admin and user portals
- Geo-redundant network for secure, reliable service

About Medtel

Medtel Communications is a pioneer in the telecommunications industry, providing a cloud-based unified communications platform that includes voice, IVR, contact center, and video conferencing solutions for businesses worldwide.

Medtel Communications

Product Line-Up and Supported Services

M-Cloud Business Phone Features	Collaboration Tools	Contact Center

• API for CRM Integration
• Automated Attendant (400 Included)
• Call Management
  • Anonymous Call Rejection
  • Call Barring, up to 7 levels
  • Call Blacklisting
  • Call Distribution
  • Call Flow Modes (Based on Bus Hours)
  • Call Forwarding
  • Call History
  • Call Hold
  • Call Listen, Intrude, and Whisper
  • Call Logging
  • Call Monitoring
  • Call Park
  • Call Pick-up/Call Pick-off
  • Call Routing
  • Call Queues
  • Call Scheduling
  • Call Transfer
  • Call Waiting (internal and external)
• Caller ID
• Chrome Web Browser Extension (softphone)
• Cloud-based PBX
• Company Directory
• Do Not Disturb
• HD Call Quality
• Hotline Button
• Hot Desking
• Hunt Groups
• Mobile App (IOS and Android)
• Multi-Device (desk phone, mobile, or web phone)
• Music on Hold
• Paging & Intercom
• Phone Programming
• Ringing Modes
• Web Phone (via Web Portal & Chrome Ext)
• Unlimited Calling US & Canada
• Voicemail (425 Boxes)
• Voicemail to Email with Transcription
• Web Portal
	• Audio Conference Bridges (Includes 2 bridges, up to 7 participants per bridge)
	  • Unique bridge number and access codes
	  • Host controls (Mute/Unmute/End)
	• Instant Messaging
	• Presence
	• Video Conferencing
	  • Up to 70 Participants
	  • Active Speaker or Mosaic View
	  • Audio Conference Bridge
	  • Bandwidth Adaptation and Reporting
	  • Click-to-Join with Web Browser (doesn't require additional software)
	  • Group and Private Chat
	  • Host Controls (Mute/Unmute/Record)
	  • Screen Sharing
	  • Send Invites to Email, Google Calendar, Office 365, or Outlook.com
	  • Video Conference Recording
	  • YouTube Broadcasting
	  • YouTube Video Sharing
		Includes All M-Cloud Business Phone Features, Plus:
		• 200 Agents
		• Agent Priority Routing
		• Agent Skill Sets, up 50
		• Agent and Supervisor Login/Out
		• Agent Wrap-up Time
		• Auto Attendant (300)
		• Advanced Call Distribution, Management, and Routing
		• Custom Hold Messages
		• Performance Indicators
		• Reporting and Analytics
		  • Skill Set/Agent Reports
		  • Longest/Average Wait Times
		  • Longest/Average Call Times
		  • Maximum Call Volume
		  • Abandoned Calls
		• Skill Set Mailboxes
		• Supervisory Tools: Listen-in, Intrude, and Whisper
		• Wall Boards with Real Time Performance Stats by Agent or by Skill Set Pool
		  • Call Queues
		  • Answered Calls
		  • Abandoned Calls
		  • Calls Answered by Voicemail
		  • Calls Forwarded
		• Web Portal

Medtel™ Communications

(Reference CRFP 1500 AGO2400000001 Section 2, Number 13) REGISTRATION Medtel Communications is Licensed in the State of West Virgina.

(Reference CRFP 1500 AGO2400000001 Section 2, Number 23) EMAIL NOTIFICATION OF AWARD. Please email jchoplin@medtelcom.com, bwebb@medtelcom.com for Notification of Award.

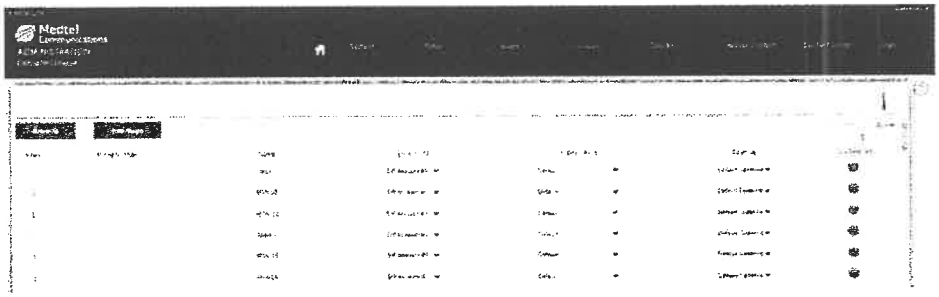
4.2.1. Goals and Objectives

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.1.1) Replace all on premise server devices with a cloud-based solution for the Agency's telephony requirements. Medtel's M-Cloud solution is cloud-based and does not require premise-based servers.

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.1.2) Maximize security against all potential information technology risks by accessing all cloud-based security capabilities relative to the solution. Please see attachment A as well as our Security Architecture document (Attachment B), and the Medtel Communications Data Protection Policy and Procedures document (Attachment C).

4.2.1.3 Acquire the most cost beneficial solution accommodating all of the needs and desires of the Agency at the time of deployment. See Medtel Pricing Attachment C

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.1.4) Automated attendant/voice menus should accommodate up to 300 numbers. MedTel's business phone system manages up to four hundred phone numbers. Capacity can be expanded beyond four hundred via networking multiple systems together.

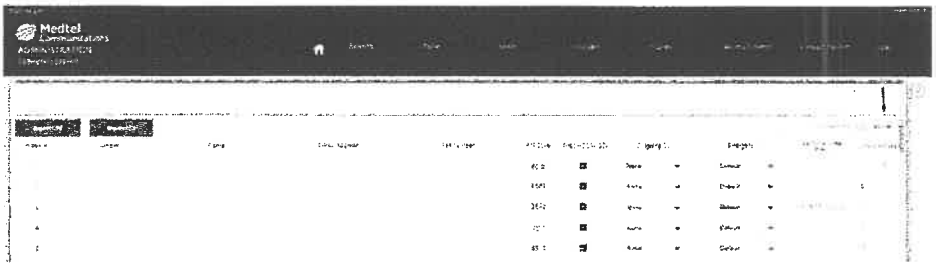


Phone number management in the M-Cloud Admin Portal

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.1.5) Contact Center should accommodate 400 agents. Medtel has systems that can accommodate 200 or 400 Contact Center Agents. In this instance, Medtel will implement the system capable of supporting 400 agents unless otherwise requested. The system can be expanded beyond 400 users by networking multiple systems together. User Licenses are enabled on the back end by a System Administrator, allowing for as many Agent Licenses as user Licenses.

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.1.6) Hunt List should accommodate up to 200 end users. Medtel's M-Cloud Groups settings can accommodate up to 200 End Users.

Medtel Communications



User management in the M-Cloud Admin Portal

4.2.2.1 Security

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.1a, 4.2.2.1b) Please see attachment A as well as our Security Architecture document (Attachment B) and Medtel Communications Data Protection Policy and Procedures document (Attachment C).

4.2.2.2 Third Party Integration

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.2) The system does not currently integrate with Microsoft Outlook. We are exploring development. However, at the time of this document, we do not have a release date. Medtel's M-Cloud system offers voicemail transcription and voicemail to email. Contact lists and employee directories formatted as .CSV files can be uploaded to the M-Cloud Admin Portal and can be accessed via desktop phone, M-Cloud User Portal, and Medtel's Mobile Application.

4.2.2.3 Agency Support

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.3) Technical Support is available, Monday through Friday from 8:00am to 8:00pm. After-hours support is available 24/7/365. All support calls received during normal business hours are handled through completion. Calls received after hours will are prioritized based upon service affecting issues, versus non-service affecting issues. Medtel resolves most service issues within our High, Medium, and Low priority policy. Service issues out of our control, such as Acts of God, Internet Provider outages, etc. may fall out of tolerance. Our Technical Support can be reached at 1-800-404-9941 or by emailing us at Techsupport@medtelcom.com. This email address automatically generates a case in Medtel's Customer Relationship Management software, thereby expediting case assignment and responses.

4.2.2.4 Training

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.4a,4.2.2.4d) User and Admin training will be completed prior to going live and can be requested with a 3–5-day notice for scheduling after a system is live. The 3–5-day notification is required to schedule training whether on-site or remote. A Library of Training Videos on all key aspects of products and features is available. The following links allow access to our Training Resources:

- For App and Web Phone training videos Please use this link: https://www.medtelcom.com/resources/training-center/
- For Insights Training Videos please use: https://www.medtelcom.com/resources/insights-training-center/
- Additional training videos https://www.medtelcom.com/resources/help-center/

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.4b, 4.2.2.4c) Medtel offers individual and group training sessions on-site and remotely. Most of our Training Sessions can be conducted

remotely. Recordings of remote training sessions can be provided as needed.

4.2.2.5 White Label Solutions Excluded

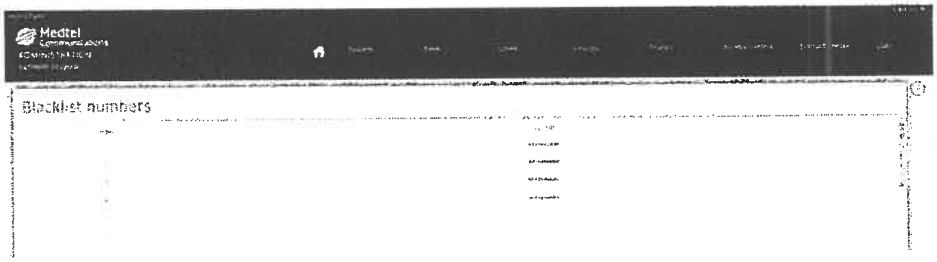
(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.5) Medtel Communications is the sole provider for design, maintenance, development, and Technical Support of our communications platform.

4.2.2.6 Vendor References

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.6) Please see the Attached Reference Documents (Attachment D)

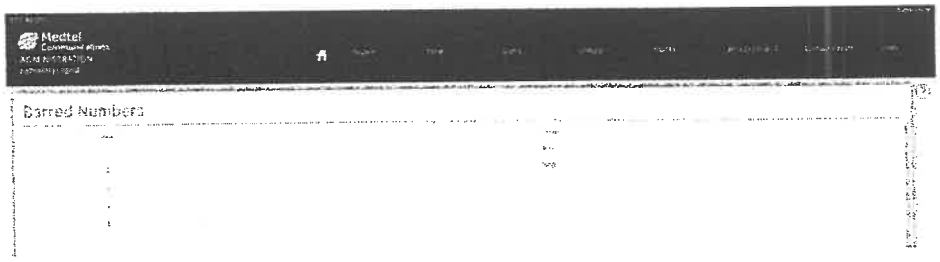
4.2.2.7 Granular Control

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.1) Blacklist Calls from Specified Numbers: The Medtel Communications VoIP system allows calls to be blacklisted, or blocked, directly from the phones themselves as well as from the Admin Portal. Numbers that were backlisted from a phone can only be removed at the phone. Once a number is added, it will remain there until removed by the user or administrator. Blacklisting prevents incoming calls.



Blacklisting numbers in the M-Cloud Admin Portal

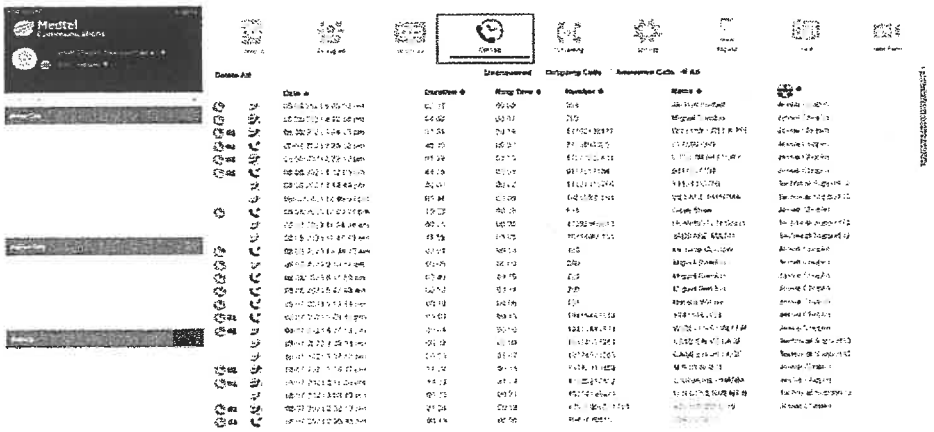
(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.2) Call Barring with up to 7 Levels: Our system allows barring numbers by entering the area code, prefix, or an exact number via the Admin Portal. We also allow restrictions based on individual phones that can restrict a phone to internal only, national, or international dialing plans. This feature only limits outbound calling. It is not a restriction for Inbound calling like Blacklisting or call blocking referenced above. Unlike Blacklisting or blocking this feature must be configured in the Admin Portal. Standard users will not have access to this feature from their phone.



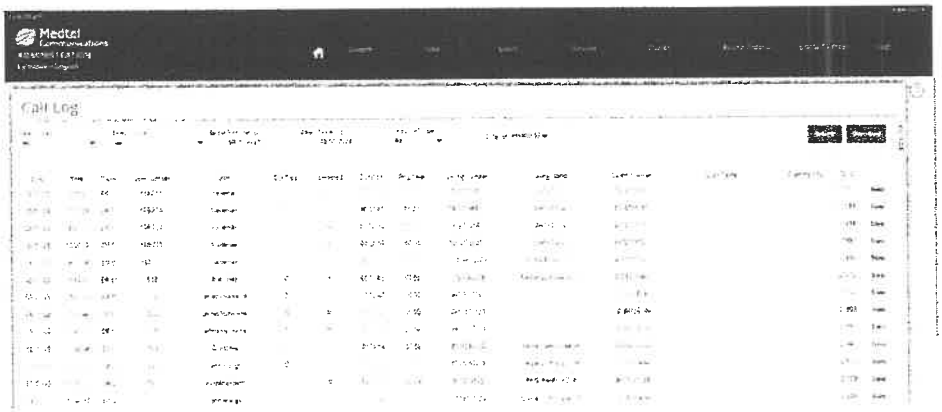
Barred Numbers in the M-Cloud Admin Portal

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.3) Call Lists (Missed, Dialed, Received): There are three ways to access this information; via the phone "History Button", the M-Cloud User Portal Call Log, or the Admin Portal Call Log. All three options are easy to retrieve

depending on user access level. Reports for missed calls, dialed calls, and received calls are all available. Each user will receive an email that gives them access to their individual M-Cloud User Portal. From the User Portal, the user will click on the Call Logs Icon. System Administrators may log into the Admin Portal and navigate to the Logs section to access these reports.



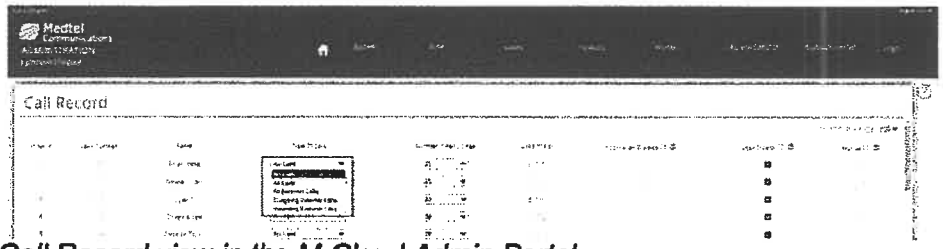
Call Log view in the M-Cloud User Portal



Call Log view in the M-Cloud Admin Portal

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.4) Call Recording: Call Recording can be enabled and managed as follows:

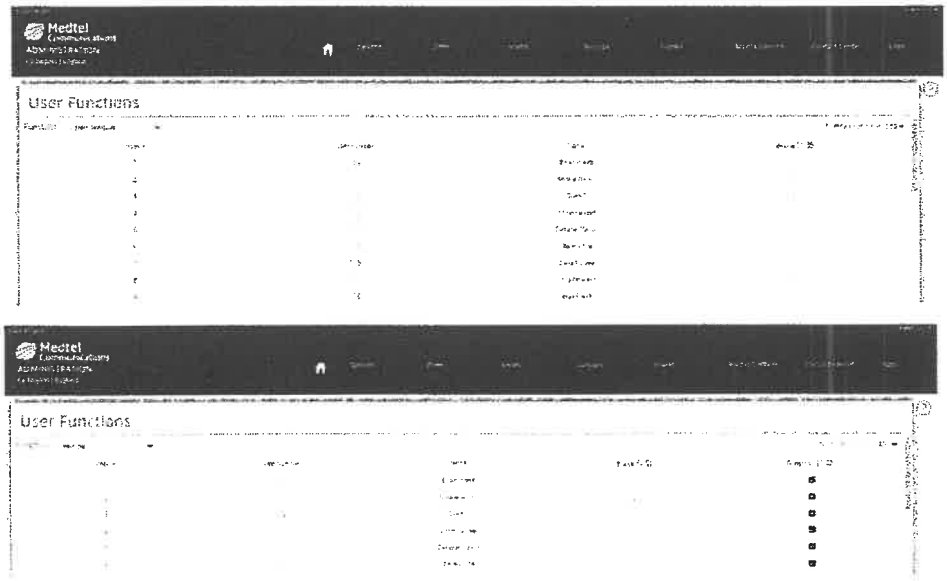
- Call Recording is enabled on an individual extension basis. The options are Inbound Only, Outbound Only, Internal Only as well as Inbound and Outbound with or without Internal calls.
- The system Admin Portal allows you to select the notification to be enabled. It beeps at the beginning of the call to alert the user that the call is being recorded. Call recording on a phone can be enabled User Control, via the Display button on the phone, can be enabled as well. This allows a user to choose what calls to record within the parameters set in the System Admin Portal.
- There are multiple ways to store recorded calls. They can be sent to an email, FTP Server (provided by the customer), or Archiving. Medtel's servers have a finite storage capacity, and an FTP storage solution is recommended.



Call Record view in the M-Cloud Admin Portal

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.5, 4.2.2.7a.6) Our system allows Listen, Whisper, and Intrude. All three features can be used independently or in conjunction with Call Recording. Permissions are set through the System Admin Portal by authorized personnel:

- The Listen feature allows you to listen to another without either party knowing. This can be accessed via the press of a button or dialing a code.
- The Whisper feature allows you to listen to the call and speak with the user without the external party hearing you. This could be used in a coaching scenario.
- The Intrude feature allows an authorized to Barge/Intrude into any call at the touch of a button or entry of a code.



Whisper and Intrude view in the M-Cloud Admin Portal

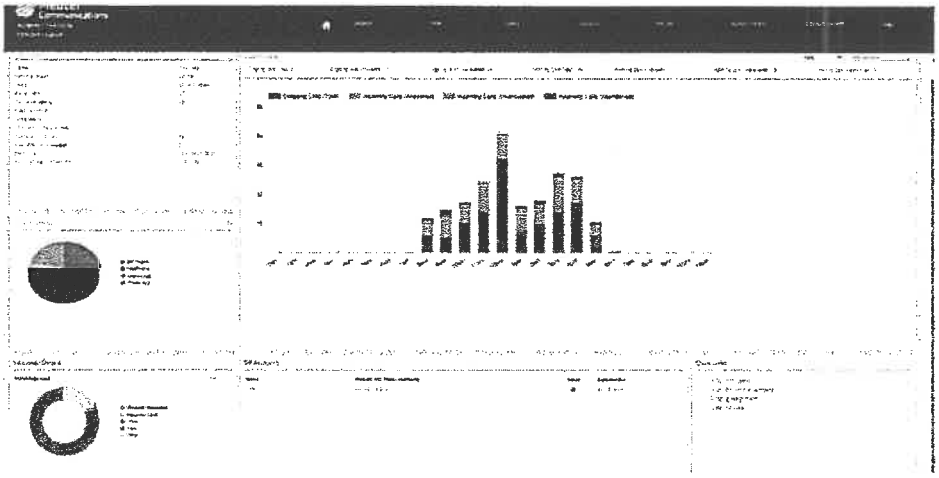
(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.7) Browser-Based System Programming: Medtel Communications System Admin portal is only accessible via web browser. Chrome is the recommended browser. System Administrators have access to the following settings in the M-Cloud Admin Portal:

- User Management: Administrators can create, modify, and delete user accounts, as well as manage their access levels and permissions.
- Call Routing: Administrators can configure call routing rules, such as call forwarding, call blocking, and caller ID settings.
- System Settings: Administrators can configure system settings, such as time and date settings, call recording settings, and network configuration.
- Voicemail Settings: Administrators can configure voicemail settings, such as voicemail

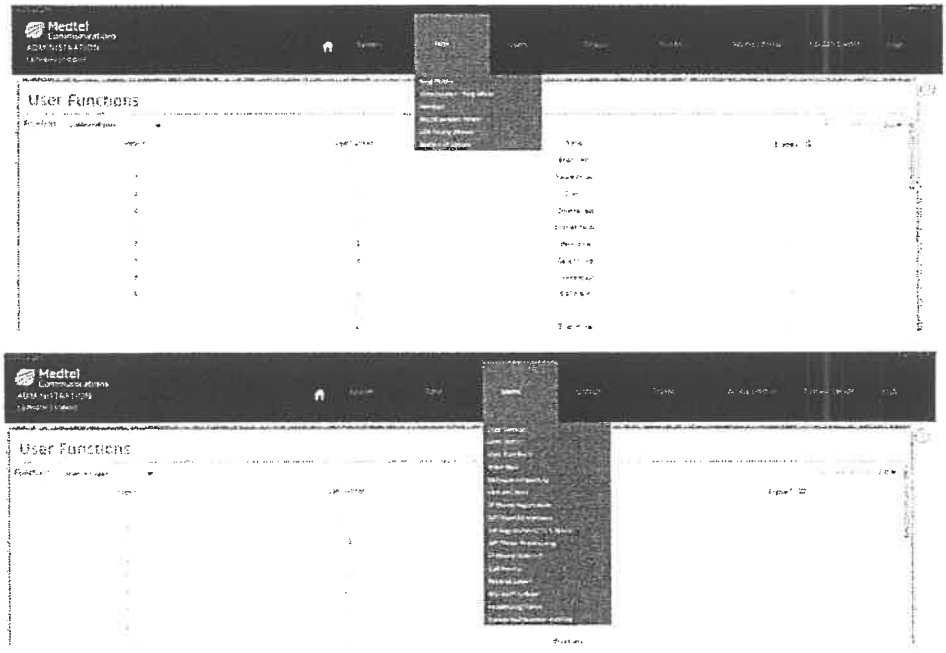
Medtel Communications

greetings, voicemail to email settings, and message playback options.

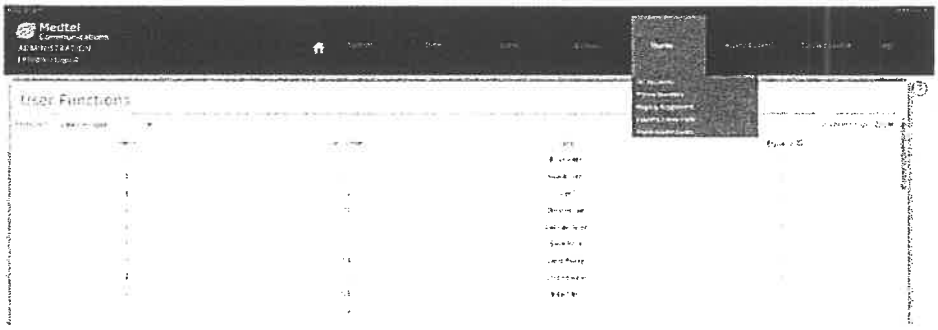
- Call Management: Administrators can manage call queues, call groups, and call center settings.
- Reporting and Analytics: Administrators can view reports and analytics on call usage, call quality, and other metrics to optimize their VoIP system's performance.
- MedTel's Admin Portal provides full control to administrators, allowing them to make administrative changes and customizations to meet the needs of the organization.



Dashboard View in the M-Cloud Admin Portal



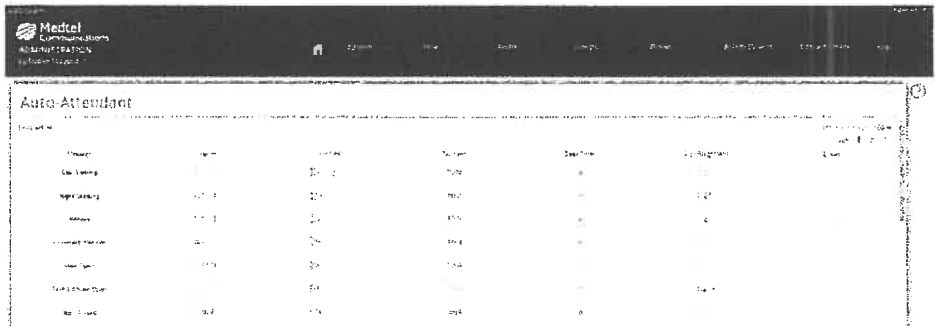
Medtel™
Communications



Medtel Communications

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.8) Attendant Console: Automated Attendant/Voice Menus: Medtel Auto Attendants are used to direct calls, external or internal, to the extension, group or skillset required. Each system has up to 400 Auto Attendants available. Each Auto Attendant allows callers to navigate through a series of pre-recorded options using their phone's keypad. With an Auto Attendant, callers can:

- Select options from a pre-recorded menu: Callers can listen to a pre-recorded menu of options and select the appropriate option by pressing a number on their phone's keypad or by using voice recognition technology.
- Receive automated responses: Callers can receive automated responses that provide them with information, such as business hours, directions, or website links.
- Be directed to the appropriate department or extension: Callers can be directed to the appropriate department or extension based on their selection or based on pre-defined rules, such as time of day or caller ID.
- Leave voicemail messages: Callers have the option to leave voicemail messages if the party is not available.



Auto Attendant View in the M-Cloud Admin Portal

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.8) Group and Skillset Features: System settings are managed in the Admin Portal. All System Administrators will be trained to make changes to the phone system. Medtel Technical Support can also be contacted to assist with programming adjustments as needed. The phone system will be designed and configured based on information specified during the system design session prior to going live.

- All Groups and Skillsets can be programmed for Ring All, Priority Routing or Cyclic Routing. They can also be programmed for different ring cadences that allows users to audibly discern call origin.
- Queues are also available, but call waiting must be disabled for this feature to work as intended. Call routing using groups and auto attendants can be configured to work like queues.
- Call routing can be programmed to accommodate different scenarios and schedules based on user availability or temporary circumstances (vacations, on-call personnel, assignments, answering services, etc.) with Auto Attendants.

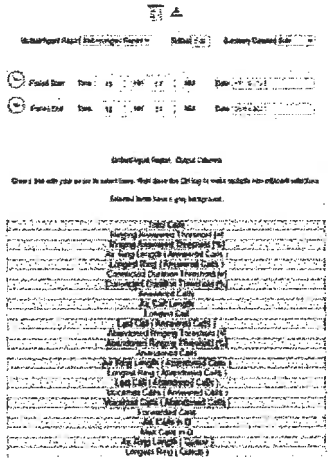
(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.9) All Reporting Features: Medtel offers multiple reporting cap:

- Contact Center Reporting allows System Administrators to view and schedule reports can be done under the Contact Center section of the System Admin as well as our reporting interface in Insights. These reports can be emailed to multiple emails or accessed immediately.
- Insights reporting offers similar options as Call Center Reporting but is viewed through Medtel

Medtel Communications

Insights, our web-based Insights Product. All reporting features cover group and extension/Agent.

- Some of the categories for our reporting include, but are not limited to, calls answered, calls missed, abandoned calls, and calls that go to voicemail.



Skillset Agent Reports in the M-Cloud Admin Portal

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.10) Import/Export of Contacts: MedTel's "Common Address Book" can be imported and exported via the System Admin Portal. A user can add common contacts and Individual contacts through their User Portal as well. Common Contacts are available to all users within the system and utilizes a .csv file. When edited and imported it will overwrite the previous Directory.

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.7a.11) SIP Trunking: A MedTel Cloud PBX can have up to 23 additional SIP Trunks. They can be used for "Trunking" to an external system or extension to extension dialing for a non MedTel System. Combined with Least Cost Routing allows a PBX to be flexible with respect to Organizations that may not have migrated their other Locations to the MedTel System. The only limitations are that of the network and phone system we are attempting to create a "trunk" with.

4.2.2.8 IP Routing / Filtering Device

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.8) Medtel's M-Cloud phone system is a cloud-based system that does not require the onsite installation of servers. Medtel's User and Admin portals are accessible via internet connection and web browser using a personal computer (PC). End users have the option of utilizing desktop phones which are connected to the system via ethernet cables, Medtel's Web Phone (accessible via internet-connected PC with web-browser), or Medtel's Mobile app installed on the end-user's mobile phone (Android and iPhone compatible).

4.2.2.9 Solution Platform Access

(Reference CRFP 1500 AGO2400000001 Section 4, 4.2.2.9) Access to development and solution platform Engineers is available and requests should be submitted via Medtel's Sales Engineer or Technical Support Management.

Medtel Communications

4.3.1. Qualification and Experience

4.3.1.1. Please provide any experience you have regarding deployment of your recommended solution to government entities.

Medtel Communications Selected to Deploy COVID-19 Emergency Contact Centers for Two County Government Offices in North Carolina

Union County Government, headquartered in Monroe, NC, supports upwards of 200,000 citizens. The county's IT Department was tasked with establishing a COVID-19 Vaccine Hotline and Contact Center for Union County Health Services.

Steve Farrell, Senior Systems Analyst for Union County, engaged Medtel Communications to build and rapidly deploy a Contact Center solution capable of processing hundreds to thousands of calls during hours of operation.

"Medtel was able accommodate our quick-turnaround time with professionalism while demonstrating a commitment to customer service." - Steve Farrell, Senior Systems Analyst for Union County

Pender County Government, headquartered in Burgaw, NC, is a government entity that supports over 52,000 residents. Pender County Health and Human Services Department had an immediate need to open a dedicated phone line for COVID-19 vaccine inquiries and appointments.

R. Earl Moore, ITS Operations Manager, and Doug Shipley from Pender County were referred to Medtel Communications by Union County officials, based on the success of their own COVID-19 Hotline. The Medtel Communications platform was the right fit for the project because it was cost-effective, easy-to-use, with appealing features and capabilities. Since the deployment, the Pender County Health Department has taken thousands of calls from residents seeking information about vaccines.

"Medtel worked with us to rapidly deploy our contact center. Within days, we were able to activate our COVID response center and begin taking calls. Medtel was there every step of the way offering advice and support. Because of this successful rollout, we are expanding with a secondary contact center for our Health Department." - R. Earl Moore, ITS Operations Manager, Pender County

Health Department Call Center
Daily Average: 185
Average Maximum Wait Time: 1 Minute
Maximum Callers in Queue: 13

Covid-19 Call Center
Daily Average: 400
Average Maximum Wait Time: 6 Minutes
Maximum Callers in Queue: 115

Medtel™ Communications

4.4. Oral Presentations

(Reference CRFP 1500 AGO2400000001 Section 4, 4.4) Medtel Communications has completed a live sales presentation, product demonstration/test system, Q&A, and product training. Additional presentations and product demonstrations can be scheduled as required.

4.5 Attendant Console/ Hunt Group

(Reference CRFP 1500 AGO2400000001 Section 4, 4.5) Medtel's business phone system manages up to 20 unique Groups and 50 Unique Skill sets per individual system. Groups and Skill set users can be programmed with Log In/Out buttons enabling the users to switch seamlessly from one to another. While they cannot be "divided" into groups and skillsets within themselves, they can be set to Ring All, Cyclic or Priority ringing.

Medtel Communications

Medtel Reliability and Redundancy

Medtel Communications provides best-in-class VoIP phone service designed to provide efficient and reliable communications solutions to businesses throughout the North America. Medtel combines multiple points of redundancy
in three key areas to ensure service dependability and 99.99% uptime.

- **Amazon AWS (Amazon Data Center)** Medtel's VoIP service is hosted with Amazon Web Services.
- **Carrier-Grade VoIP Origination** Medtel offers local and toll-free numbers from the largest DID network in North America, backed by a fully redundant voice network.
- **Medtel M-Cloud Service** Medtel's proprietary purpose-built platform is a dependable and stable communications network.

Amazon AWS Redundancy

AWS utilizes multiple data centers for physical location redundancy. AWS provides one connection at multiple locations for critical production workloads that require high resiliency. If a data center has an issue affecting even a small percent of users, calling automatically fails over to the nearest location, so that customers are not impacted.

PSTN Redundancy

Our PSTN carrier offers several different origination and termination IP addresses for connectivity. If the primary connection fails, our M-Cloud PBX will communicate to the carrier through pre-designated secondary connections. In addition to this redundancy, our carrier provides a "Fail Over" number in case of a connection failure via any of the redundant IP addresses.

Virtual Machine (VM) Level Redundancy

All M-Cloud systems are hosted on Virtual Machines within Amazon Data Centers. Medtel's VMs (Virtual machines) are backed up every 15 minutes. In the event of a server failure or any other VM-related issue, Medtel can load the latest backup on a new VM and restore system functions within minutes.

Endpoint Level Redundancy

Each extension in an M-Cloud PBX can forward to a destination if that endpoint cannot register to the PBX for any reason. Some common reasons for a device's failure to register might be an unplugged phone, a bad data connection, a power outage, or a failure to reach the internet on the local LAN or through the customer ISP. Calls can be forwarded to any valid destination if a phone cannot be registered such as: a voice mailbox, cell phone number, another extension, or to an answering service.

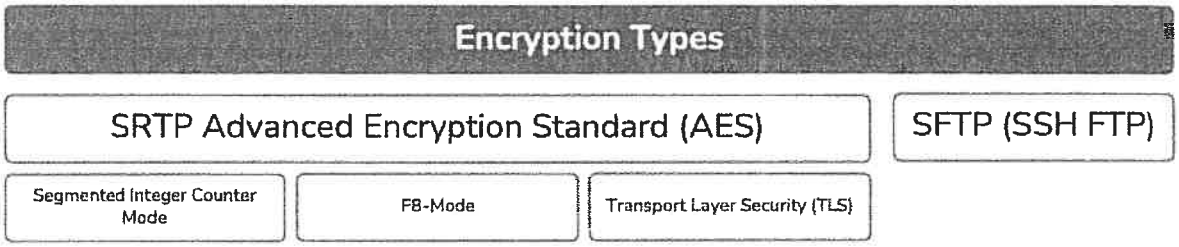
Customer's Connectivity

The two variables in the connection equation inherent in cloud PBX technology are the customer's local office/store network and their ISP (Internet Service Provider). Since these are owned and operated by the customer or by vendors supplying services to the customer, redundancy in these areas is not under Medtel's control. Medtel Communications will make recommendations to the customer based on best practices to ensure quality and uptime standards are maintained with minimal service disruptions.

Medtel™ Communications

Enterprise-Grade Security

Medtel's comprehensive approach to security utilizes the Amazon Web Services (AWS) Platform. Your data is protected by 256-bit Advanced Encryption Standard inside redundant storage at several physical locations for both security and availability purposes. Since our team also monitors threats and audits our systems around the clock, you'll never need to worry about a data breach.



Call Encryption

Calls are made using WebRTC technology, which means signaling for call setup is executed using WebSockets via TLS to provide complete privacy and data integrity. As soon as the call starts and someone begins speaking, voice packets are encoded in SRTP (Secure Real-Time Protocol). It ensures encryption, message authentication, integrity, and replay protection so that any sniffed packets cannot be deciphered. Overall, your VoIP calls are safer and more secure than calls over a traditional phone network.

FTP Encryption

SFTP, also known as SSH FTP, encrypts both commands and data while in transmission. This means all your data and credentials are encrypted as they pass through the internet. SSH is a protocol that allows you to remotely connect to other systems and execute commands from the command line. SSH is how most servers in the world are administered, so the protocol is very secure. SFTP was created as an extension of SSH to transfer files through the secure channel (SSH).

Medtel Communications

Medtel Communications – Customer Examples

Allen Industries
Your Complete Signage and Architectural Element Expert

Firkins AUTOMOTIVE

HEART SPECIALISTS OF SARASOTA

InfuCare Rx

LeMed SPECIALTY PHARMACY

1870 AD MAJOREM DEI GLORIAM | LOYOLA MEDICINE

Osborn Drugs
a ProRx Pharmacy

UNIVERSITY of MARYLAND MEDICAL CENTER

Medtel Communications

4.2.2.1 Security
Medtel Communications

ATTACHMENT A

1. **How do you protect against unauthorized access to the VoIP system and its data?**

   In addition to the standard AWS data protection mechanisms, a combination of encrypted usernames and passwords and Medtel Cloud whitelists and blacklists protect against unauthorized access at the User, Admin, and Installer levels. Please see the attached Security Architecture document for further detail. (Attachment B)

2. **What measures do you have in place to prevent hacking and other cyberattacks on the VoIP system?**

   Hacking and other cyberattacks are prevented by a combination of encrypted usernames and passwords and Medtel Cloud whitelists and blacklists. After three false registration attempts or an excessive amount of registration attempts in a short amount of time, also known as a brute force attack, access to that particular portal form the offending IP Address is blocked. Please see the attached Security Architecture document for further detail. (Attachment B)

3. **What is your disaster recovery and business continuity plan in case of a cybersecurity incident?**

   The Medtel Disaster recovery and business continuity plan is attached. (Attachment E)

4. **What encryption standards do you use to secure voice and data traffic?**

   The encryption standards used are listed in the Security Architecture document attached. (Attachment B)

5. **Do you perform regular security assessments and audits of your VoIP system?**

   Medtel performs regular security assessments and audits of the Medtel Cloud platform. Addresses from which cyber-attacks are detected are automatically blacklisted.

6. **Do you have a dedicated security team that monitors the VoIP system and responds to security incidents?**

   The Medtel Data Protection Officer chairs quarterly security meetings.

7. **How do you ensure compliance with industry regulations such as GDPR, HIPAA, or PCI DSS?**

   The Medtel Communications Data Protection Policy and Procedures document is attached.

Medtel Communications

(Attachment C)

8. **What are your policies and procedures for handling and securing sensitive customer data?**

   Procedures are described in the attached Medtel Communications Data Protection Policy and Procedures. (Attachment C)

9. **What authentication and access controls do you have in place to restrict access to the VoIP system?**

   Authentication and access controls are described in the attached Security Architecture - Medtel Cloud PBX document. (Attachment B)

10. **Can you provide evidence of your security certifications and compliance with industry standards?**

    Medtel Cloud PBX is hosted in the AWS environment where the highest security standards apply.

Medtel Communications

4.2.2.1 Security
Security Architecture – Attachment B
Medtel Cloud PBX / Contact Center

1. System Architecture

The Medtel platform is a Unified Communications/ Cloud PBX platform normally hosted on Amazon AWS US East (N.Virginia) or AWS US West (Oregon). It consists of multiple Linux based (Rocky 8) virtual machines with fixed IP4 addresses which are accessible via the Linux VM firewall and the individual cloud PBX firewall.

Each PBX on the VM has a unique name (usually the customer's name). DNS is used to associate each PBX name with the correct VM.

Connectivity to the Public switched network is normally via VoIP Innovations SIP trunks. SIP trunks can connect using SIP Registration. In cases where registration is not used, whitelisted IP addresses are specified for the trunk.

- End-Users connect to the PBX using:
- Browser based web phone
- iPhone / Android app (over Wifi / 4G)
- SIP deskphone / applications

2. VM Management

VM management can be divided into 2 sections.

2.1 VM Command Line access via SSH

- SSH access (username / password login required) to each VM is limited (via the primary firewall) to a small number of IP addresses. Command line access is used to:
- Start / stop / upgrade firmware on the VM.
- Create / Delete / Update / Manage PBXs on the VM.
- Enable / Disable services (SOAP API / Call Log API etc)
- Set credentials for Master Installers.
- Set Whitelist IP addresses for Master Installers, remote SOAP / Call Log clients etc)

2.2 Master Installer Portal

The 'Master Installer Portal' is accessible via https and gives access to all Cloud PBXs running on the VM. Usernames and passwords for Master Installer access are set via command line. Access is also limited to predefined whitelisted IP addresses (also set via the command line). A Master Installer cannot change their password.

Medtel Communications

3. **PBX / User Management**
The PBX Management Portal is used to manage a single PBX. It is used to create / delete / edit Users, Configure SIP trunks, Manage the PBX firewall etc.
There are 6 classes of user that can manage a single PBX:
    - Install
    - Admin
    - Admin2
    - Admin3
    - Admin4
    - Admin5

    Each login is password protected (randomly generated when PBX is created). Once logged in, a user may change their password. A Master Installer may also change the password for each of these users. The 'install' user has access to all parameters / PBX logfiles within the PBX (SIP trunk details, User details etc). The admin users have restricted access. The features that each admin has access to is set via a config file only accessible via the command line.

    Typical data required when creating a new user is:
    - Extension Number
    - Users Name (This name is used to log in to the Users portal as detailed in section 4)
    - Email address
    - Pincode (Min 4 digits, Max 8 digits)

4. End User Access

Each user on the cloud PBX has access to their own portal where they can manage their settings, make calls, set call-forwarding, view/download voicemails etc. A username & PIN are required to log in. Each user may change their own PIN.
The functionality available to each user may be restricted by the install / admin users.

5. Firewall Protection

There are 3 levels of Firewall protection.
- Primary Firewall: This is the AWS Firewall which sits between the hosting environment and the public internet.
- VM Firewall: Each VM runs Rocky 8 which includes a Firewall to control access to the VM.
- PBX Firewall: Each PBX can restrict access to its own services.

6. Device Registration

A user needs to register their device (Web phone SIP Phone / Smartphone app) before being able to make / receive calls. Random registration names & PINS for all Users are generated when a PBX is created.
- Web Phone. When a user is created by the administrator, a welcome email can be sent by the system to the user with a link to open their user portal directly.

Medtel Communications

- SIP Phones and Smartphone Apps may be provisioned automatically:
- SIP Phones: provisioned on power-up based on device MAC address and User-Agent string via built in provisioning server.
- Smatrphone Apps: provisioned using random pairing code (only valid for 120 seconds after provisioning request is made via User Portal)

7. Logging

All debug logfiles are held locally on the VM. A Master Installer has access to all logfiles on the VM. A PBX installer only has access to logfiles for a single PBX.
Call records may be stored locally on VM in db / text file. Alternatively, they may be stored remotely on a MySQL db.

8. External Interfaces

The following gives a summary of all external interfaces to/from the Medtel platform:

Interface	Protocol	Function
Browser Access	https (port 443)	Master Installer / PBX Installer / User Portal
Smartphone Apps	TCP 5075 (Encrypted AES-128) / WSS	Proprietary Signalling
	RTP (Encrypted AES-128)	Media stream
SIP Endpoints	SIP (UDP/TCP/TLS/WSS)	SIP Device Signalling
	RTP / STRP	SIP Device Media
Browser SIP Endpoints	SIP (WSS)	Browser based SIP Signalling
	WebRTC (DTLS)	Browser based SIP Media
SIP Trunks	SIP (UDP)	SIP Trunk Signalling
	RTP	SIP Trunk Media
Manager	SSH	Command Line Management
Provisioning	HTTPS	SIP Device / Smartphone provisioning (Note 1)
xHTML	HTTPS	SIP Device Microbrowsers (Menu / Function key functionality) (Note 1)
CTI	HTTPS	External CRM integration (Note 1)
Email	SMTP (TLS)	Sending voicemail / welcome emails
FTP	FTP/SFTP/FTPS	Remote storage of voicemails / recordings
Call Logging	TCP	Third party Call log retrieval (Note 1)
SOAP	HTTPS	Third party management of PBXs (Note 1)

Notes:
Managed via PBX Management Portal may be enabled / disabled. If enabled, can be limited to Whitelist IP.

9. Mobile Applications Privacy

The Medtel mobile apps allow users access their contact lists on their devices (iPhone or Android), for the purpose of making calls. The Medtel platform does not take a copy of the contact list.

Medtel Communications

10. Customer Interfaces Security

Firmware: 22.XXX		
Customer interfaces security		
	Media stream	**Signalling stream**
Smart phone app, iPhone	AES-128	Stream AES-128. Registration: Name/Password. 2-step: browser log in and key generation
Smart phone app, Android	AES-128	Stream AES-128. Registration: Name/Password. 2-step: browser log in and key generation
Windows PC softphone	AES-128	Stream AES-128. Registration: Name/Password protected.
Desk top phone Yealink	SRTP	Stream TLS. Registration: Name/Password protected.
Desk top phone Polycom	SRTP	Stream TLS. Registration: Name/Password protected.
Web based user portal	Web RTC	SIP over WSS (secure web socket - TLS)
Chrome extension	not applicable	WSS (secure web socket - TLS)
Video collaboration	Web RTC, peer-to-peer	Web RTC, peer-to-peer
Management		
Access to the installer/system manager portal	not applicable	HTTPS - User name and password log in. Whitelist IP address option.
Access to the master installer portal	not applicable	HTTPS - User name and password log in. Whitelist IP address required.
GDPR		
Smart phone apps	not applicable	Smart phone Contact list not copied to the platform; accessed locally by app.
User portal	not applicable	All data entered and removed by the user.
System manager portal	not applicable	All data entered and removed by the system manager.

Medtel™ Communications

4.2.2.1 Security

Medtel Communications Attachment C
Data Protection Policy & Procedures

1 Policy Statement

Medtel Communications (hereinafter referred to as the "Company") needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes (but is not limited to), name, address, email address, data of birth, IP address, identification numbers, private and confidential information, sensitive information and bank/credit card details.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the General Data Protection Regulation (GDPR) and any other relevant data protection laws and codes of conduct (herein collectively referred to as "the data protection laws"). The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, procedure documents, audit measures and assessments.

Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a 'Privacy by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2 Purpose

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3 Scope

This policy applies to all staff within the Company (meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company in the United States or overseas). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 Definitions

- "Biometric data"means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm

Medtel™ Communications

the unique identification of that natural person, such as facial images or dactyloscopic data.

- "Binding Corporate Rules" means personal data protection policies which are adhered to by the Company for transfers of personal data to a controller or processor in one or more third countries or to an international organization.
- "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- "Data controller" means, the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "Data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "Data protection laws" means for the purposes of this document, the collective description of the GDPR and any other relevant data protection laws that the Company complies with.
- "Data subject" means an individual who is the subject of personal data
- "GDPR" means the General Data Protection Regulation (EU) (2016/679)
- "Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
- "Personal data" means any information relating to an identified or identifiable natural person('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- "Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to

Medtel Communications

the purposes of the processing.

- "Supervisory Authority" means an independent public authority
- "Third Party" means a natural or legal person, public authority, agency or body other than the data subject, under our direct authority

3.2 General Data Protection Regulation (GDPR)

As the Company processes personal information regarding individuals (data subjects), we are obligated under the General Data Protection Regulation (GDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

3.2.1 Personal Data

Information protected under the GDPR is known as "personal data" and is defined as:

"Any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."
The Company ensures that a high level of care is afforded to personal data falling within the GDPR's 'special categories' (previously sensitive personal data), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

In relation to the 'Special categories of Personal Data' the GDPR advises that:

"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies."

3.2.2 The GDPR Principles

Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy')
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in

Medtel Communications

accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the data protection laws principles' ('accountability') and requires that firms show how they comply with the principles, detailing and summarising the measures and controls that they have in place to protect personal information and mitigate the risks of processing.

3.3 US Data Protection Authority

At the federal level, the US Federal Trade Commission (FTC) uses its authority to protect consumers against unfair or deceptive trade practices, to take enforcement actions against businesses for materially unfair privacy and data security practices.

3.4 Data Protection Officer

Where the Company has appointed a designated DPO, we have done so in accordance with the GDPR requirements and have ensured that the assigned person has an adequate and expert knowledge of data protection law. They have been assessed as being fully capable of assisting the Company in monitoring our internal compliance with the Regulation and supporting and advising employees and associated third parties with regards to the data protection laws and requirements.

4 Objectives

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have stringent measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.
The Company ensures that: –

- We protect the rights of individuals with regards to the processing of personal information
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws
- Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles
- Personal data is only processed where we have verified and met the lawfulness of processing requirements
- We only process special category data in accordance with the GDPR requirements
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested

Medtel Communications

- All employees are competent and knowledgeable about their GDPR obligations and are provided with in-depth training in the data protection laws, principles, regulations and how they apply to their specific role and the Company
- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws
- We maintain a continuous program of monitoring, review and improvement with regards to compliance with the data protection laws and to identify gaps and non-compliance before they become a risk, affecting mitigating actions where necessary
- We monitor the Supervisory Authority, European Data Protection Board (EDPB) and any GDPR news and updates, to stay abreast of changes, notifications and additional requirements
- We have robust and documented Complaint Handling and Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws and performs specific duties as set out under Article 37 of the GDPR
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance
- We provide clear reporting lines and supervision with regards to data protection
- We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes
- Any information provided to an individual in relation to personal data held or used about them, with be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language
- Employees are aware of their own rights under the data protection laws and are provided with the Article 13/14 information disclosures in the form of a Privacy Notice
- Where applicable, we maintain records of processing activities in accordance with the Article 30 requirements
- We have developed and documented appropriate technical and organizational measures and controls for personal data security and have a robust Information Security program in place

5 Governance Procedures

5.1 Accountability & Compliance

Medtel Communications

Due to the nature, scope, context and purposes of processing undertaken by the Company, we carry out frequent risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have implemented adequate and appropriate technical and organizational measures to ensure the safeguarding of personal data and compliance with the data protection laws and can evidence such measures through our documentation and practices.

Our main governance objectives are to:

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance and ensure that the designated person(s) has sufficient access, support and budget to perform the role
- Identify, create and disseminate the reporting lines within the data protection governance structure

The technical and organizational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated information security policies.

5.1.1 Privacy by Design

We operate a 'Privacy by Design' approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures (detailed below), that help us enforce this ethos.
Data Minimization

Under Article 5 of the GDPR, principle (c) advises that data should be 'limited to what is necessary', which forms the basis of our minimalist approach. We only ever obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.
Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimization enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes:

- Electronic collection(i.e. forms, website, surveys etc) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include'optional'fields, as optional denotes that it is not necessary to obtain
- Physical collection(i.e. face-to-face, telephone etc) is supported using scripts and internal forms where the required data collection is ascertained using predefined fields. Again, only that which is relevant and necessary is collected
- We have SLA's and bespoke agreements in place with third-party controllers who send us personal information (either in our capacity as a controller or processor).These state that

Medtel™ Communications

only relevant and necessary data is to be provided as it relates to the processing activity we are carrying out

- We have documented destruction procedures in place where a data subject or third-party provides us with personal information that is surplus to requirement

- Forms, contact pages and any documents used to collect personal information are reviewed every 3-months to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

Pseudonymisation
We utilise pseudonymisation where possible to record and store personal data in a way that ensures it can no longer be attributed to a specific data subject without the use of separate, additional information (personal identifiers). Encryption and partitioning is also used to protect the personal identifiers, being kept separate from the pseudonymised data sets.

When using pseudonymisation, we ensure that the attribute(s) being removed and replaced, are unique and prevent the data subject from being identified through the remaining markers and attributes. Pseudonymisation can mean that the data subject is still likely to be identified indirectly and as such, we use this technique in conjunction with other technical and operational measures of risk reduction and data protection.

Encryption
We utilise encryption as a further risk prevention measure for securing the personal data that we hold. Encryption with a secret key is used to make data indecipherable unless decryption of the dataset is carried out using the assigned key.

We utilise encryption via secret key for transferring personal data to any external party and provide the secret key in a separate format. Where special category information is being transferred and/or disclosed, the Data Protection Officer is required to authorise the transfer and review the encryption method for compliance and accuracy.

Encryption is delivered with Eset Deslock + and where necessary Windows Bitlocker.

Restriction
Our Privacy by Design approach means that we use company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Company's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by staff members who are obligated to perform processing as part of the customer service or development team.

Hard Copy Data
Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is only available in a paper format without pseudonymising options. Where this is necessary, we utilise a tiered approach to minimise the information we hold and/or the length of time we hold it for. Steps include: –

- In the first instance, we always ask the initial data controller to send copies of any personal information records directly to the data subject

- Where step 1 is not possible or feasible, we will obtain a copy of the data and if applicable

Medtel Communications

redact to ensure that only the relevant information remains (e. when the data is being passed to a third-party for processing and not directly to the data subject)

- When only mandatory information is visible on the hard copy data, we utilise electronic formats to send the information to the recipient to ensure that encryption methods can be applied (e. we do not use the postal system as this can be intercepted).
- Recipients (e. the data subject, third-party processer) are reverified and their identity and contact details checked
- Once confirmation has been obtained that the recipient has received the personal information, where possible (within the legal guidelines and rules of the data protection laws), we destroy the hard copy data and delete the sent message
- If for any reason a copy of the paper data must be retained by the Company, we use a physical safe to store such documents as opposed to our standard archiving system

5.1.2 Data Protection Audit

The policy of the Company is to carry out company wide data protection audits to better enable us to record, categorise and protect the personal data that we hold and process. The aim of the audit audit is to identify, categorise and record all personal information obtained, processed and shared by the Company in the capacity of controller/processor and to compile on a central register such information which includes: –

- What personal data we hold
- Where it came from
- Who we share it with
- Legal basis for processing it
- What format(s) is it in
- Who is responsible for it?
- Disclosures and Transfers

5.2 Legal Basis for Processing (Lawfulness)

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Article 6 of the GDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our information audit register and in our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: –

Medtel Communications

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).

5.2.1 Processing Special Category Data

Special categories of Personal Data are defined in the data protection laws as:

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited – unless one of the Article 9 clauses applies.

Where the Company processes any personal information classed as special category or information relating to criminal convictions, we do so in accordance with Article 9 of the GDPR.
We will only ever process special category data where: –

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest

Medtel Communications

- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Processing is necessary for reasons of public interest in the area of public health
- Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)

Where the Company processes personal information that falls into one of the above categories, we have adequate and appropriate provisions and measures in place prior to any processing. Measures include: –

- Verifying our reliance on Article 9(1) GDPR prior to processing
- Documenting the Article 6(1) legal basis relied upon from processing on our Processing Activities Register (where applicable)
- Having an appropriate policy document in place when the processing is carried out, specifying our: –
- procedures for securing compliance with the data protection laws principles
- policies as regards the retention and erasure of personal data processed in reliance on the condition
- retention periods and reason (i.e. legal, statutory etc)
- procedures for reviewing and updating our policies in this area

Please refer to our Retention & Erasure Policy for further guidance and procedures.

5.2.2 Records of Processing Activities

As an organization that processes personal & special category data which could result in a risk to the rights and freedoms of individual the Company maintains records of all processing activities and maintains such records in writing, in a clear and easy to read format and readily available to the Supervisory Authority upon request.
Acting in the capacity as a controller (or a representative), our internal records of the processing activities carried out under our responsibility, contain the following information: –

- Our full name and contact details and the name and contact details of the Data Protection Officer. Where applicable, we also record any joint controller and/or the controller's representative
- The purposes of the processing
- A description of the categories of data subjects and of the categories of personal data
- The categories of recipients to whom the personal data has or will be disclosed(including any recipients in third countries or international organizations)

Medtel Communications

- Where applicable, transfers of personal data to a third country or an international organization(including the identification of that third country or international organization and where applicable, the documentation of suitable safeguards)
- Where possible, the envisaged time limits for erasure of the different categories of data
- A general description of the processing security measures as outlined in section 12 of this document(pursuant to Article 32(1) of the data protection laws)

Acting in the capacity as a processor (or a representative), our internal records of the categories of processing activities carried out on behalf of a controller, contain the following information: –

- The full name and contact details of the processor(s) and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- The categories of processing carried out on behalf of each controller
- Where applicable, transfers of personal data to a third country or an international organization(including the identification of that third country or international organization and where applicable, the documentation of suitable safeguards)
- A general description of the processing security measures as outlined in section 13 of this document(pursuant to Article 32(1) of the data protection laws)

5.3 Third-Party Processors

The Company utilise external processors for certain processing activities (where applicable). We use information audits to identify, categorise and record all personal data that is processed outside of the company, so that the information, processing activity, processor and legal basis are all recorded, reviewed and easily accessible. Such external processing includes (but is not limited to): –

- IT Systems and Services
- Legal Services
- Debt Collection Services
- Human Resources
- Payroll
- Hosting or Email Servers
- Credit Reference Agencies
- Direct Marketing/Mailing Services

We have strict due diligence and Know Your Customer procedures and measures in place and review, assess and background check all processors prior to forming a business relationship. We obtain company documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

Medtel™ Communications

We audit their processes and activities prior to contract and during the contract period to ensure compliance with the data protection regulations and review any codes of conduct that they are obligated under to confirm compliance.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We draft bespoke Service Level Agreements (SLAs) and contracts with each processor as per the services provided and detail: –

- The processors data protection obligations
- Our expectations, rights and obligations
- The processing duration, aims and objectives
- The data subjects' rights and safeguarding measures
- The nature and purpose of the processing
- The type of personal data and categories of data subjects

Each of the areas specified in the contract are monitored, audited and reported on. Processors are notified that they shall not engage another processor without our prior specific authorisation and any intended changes concerning the addition or replacement of existing processors must be done in writing, in advance of any such changes being implemented.

The Processor Agreement and any associated contract reflects the fact that the processor: –

- Processes the personal data only on our documented instructions
- Seeks our authorisation to transfer personal data to a third country or an international organization (unless required to do so by a law to which the processor is subject)
- Shall inform us of any such legal requirement to transfer data before processing
- Ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- Takes all measures to security the personal data at all times
- Respects, supports and complies with our obligation to respond to requests for exercising the data subject's rights
- Assists the Company in ensuring compliance with our obligations for data security, mitigating risks, breach notification and privacy impact assessments

Medtel™ Communications

- When requested, deletes or returns all personal data to the Company after the end of the provision of services relating to processing, and deletes existing copies where possible
- Makes available to the Company all information necessary to demonstrate compliance with the obligations set out in the agreement and contract
- Allows and supports audits, monitoring, inspections and reporting as set out in the contract
- Informs the Company immediately of any breaches, non-compliance or inability to carry out their duties as detailed in the contract

5.4 Data Retention & Disposal

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion, hard drive destruction) and prioritises the protection of the personal data in all instances.

Please refer to our Data Retention policy

6 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Company. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we utilise proportionate methods to map out and assess the impact ahead of time.

Where the Company act as the Controller and must or are considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, we always carry out a Data Protection Impact Assessment (DPIA) (sometimes referred to as a Privacy Impact Assessment).

Pursuant to Article 35(3) and Recitals 84, 89-96, we consider processing that is likely to result in a high risk to include: –

- Systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person(s)
- Processing on a large scale of special categories of data
- Processing on a large scale of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale (i.e. CCTV)
- Where a processing operation is likely to result in a high risk to the rights and freedoms of an individual

Medtel™
Communications

- Those involving the use of new technologies
- New processing activities not previously used
- Processing considerable amounts of personal data at regional, national or supranational level, which could affect many data subjects
- Processing activities making it difficult for the data subject(s) to exercise their rights

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. It is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

- The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: –
- Eliminated
- Reduced
- Accepted

Please refer to our external DPIA Procedures for further details.

7 Data Subject Rights Procedures

7.1 Consent & The Right to be Informed

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the Company and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.
The data protection law defines consent as; 'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.
Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to ensure that:

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand
- Pre-ticked, opt-in boxes areneverused

Medtel Communications

- Where consent is given as part of other matters (e. terms & conditions, agreements, contracts), we ensure that the consent is separate from the other matters and isnotbe a precondition of any service (unless necessary for that service)
- Along with our company name, we also provide details of any other third party who will use or rely on the consent
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum:
- that the individual has consented to the use and processing of their personal data
- that the individual has been advised of our company name and any third party using the data
- what the individual was told at the time of consent
- how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: –
- Opt-out links in mailings or electronic communications
- Opt-out process explanation and steps on website and in all written communications
- Ability to opt-out verbally, in writing or by email
- Consent withdrawal requests are processed immediately and without detriment
- Controls and processes have been developed and implemented to refresh consent, especially those relating to parental consents
- For special category data, the consent obtained is explicit(stated clearly and in detail, leaving no room for confusion or doubt) with the processing purpose(s) always being specified

7.1.1 Consent Controls

The Company maintain rigid records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.
Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorised by the Data Protection Officer prior to being circulated.

Medtel Communications

Consent to obtain and process personal data is obtained by the Company through: –

- Face-to-Face
- Telephone
- In Writing
- Email/SMS
- Electronic(i.e. via website form)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism. Where consent is obtained verbally, we utilise scripts, checklists to ensure that all requirements have been met and that consent is obtained compliantly and can be evidenced.

Electronic consent is always by a non-ticked, opt-in action (or double opt-in where applicable), enabling the individual to provide consent after the below information has been provided. This is then followed up with an email, SMS or written confirmation of the consent to process, store and share the personal information.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

7.1.2 Alternatives to Consent

The Company recognise that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.
When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are a factor: –

- Where we ask for consent but would still process it even if it was not given(or withdrawn).If we would still process the data under an alternative lawful basis regardless of consent, we recognise it is not the correct lawful basis to use
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate
- Where there is an imbalance in the relationship, i.e. with employees

7.1.3 Information Provisions

Where personal data is obtained directly from the individual (i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc)), we provide the below information in all instances, in the form of a privacy notice: –

- The identity and the contact details of the controller and, where applicable, of the controller's representative

- The contact details of our data protection officer
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- Where the processing is based on point (f) of Article 6(1)"processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party",details of the legitimate interests
- The recipients or categories of recipients of the personal data(if applicable)
- If applicable, the fact that the Company intends to transfer the personal data to a third country or international organization and the existence/absence of an adequacy decision by the Commission
- where the Company intends to transfer the personal data to a third country or international organization without an adequate decision by the Commission, reference to the appropriate or suitable safeguards the Company has put into place and the means by which to obtain a copy of them or where they have been made available
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- Where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- The right to lodge a complaint with the Supervisory Authority
- Whether providing personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- The existence of any automated decision-making, including profiling, as referred to in Article 22(1) and (4) and explanatory information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the date of consent, unless there is a legal requirement to keep the information longer.

7.2 Privacy Notice

The Company defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly).

Medtel™ Communications

Our Privacy Notice includes the Article 13 (where collected directly from individual) or 14 (where not collected directly) requirements and provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.
We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is the customer facing policy that provides the legal information on how we handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection: –

- Via our website
- Linked to or written in full in the footer of emails
- Worded in full in agreements, contracts, forms and other materials where data is collected in writing or face-to-face
- In employee contracts and recruitment materials
- Verbally via telephone or face-to-face
- Printed media, adverts and financial promotions
- Digital Products/Services

With lengthy content being provided in the privacy notice and with informed consent being based on its contents, we have tested, assessed, and reviewed our privacy notice to ensure usability, effectiveness and understanding.

We follow the below preferred steps for testing, reviewing and auditing our privacy notice(s) and opt-in consent formats prior to use and to record such assessments.

1. Privacy Notices are drafted by the Data Protection Officer using the data protection laws requirements and with Supervisory Authority guidance
2. We utilise a select customer base to test the Privacy Notice in its varying formats and provide a feedback form for completion, verifying the below points: –

1. How did you use the Privacy Notice (e.g. website, agreement, orally)?
2. Did you find the information in the Privacy Notice easy to read, understand and access?
3. Did you gain a full understanding of how we intend to use your data, who it will be shared with and what your rights are?
4. Did you feel confident in giving consent to use your personal data after reading the notice information?
5. Was there anything you did not understand?
6. Did you find any errors?
7. What, if anything, would you like to see changed about the Privacy Notice?
8. All feedback responses are saved with a copy of the used Privacy Notice and improvements are made and recorded where applicable
9. Re-testing is carried out on a new set of customers to ensure variety and independent assessment and verification
10. After a successful test, the acceptable Privacy Notice is rechecked against the data protection laws and Supervisory Authority regulations and guidelines to ensure it still complies and is adequate and effective
11. The final Privacy Notice(s) are then authorised by Senior Management/Director(s) before

being rolled out

Where we rely on consent to obtain and process personal information, we ensure that it is:

- Displayed clearly and prominently
- Asks individuals to positively opt-in
- Gives them sufficient information to make an informed choice
- Explains the different ways we will use their information
- Provides a clear and simple way for them to indicate they agree to different types of processing
- Includes a separate unticked opt-in box for direct marketing

7.3 Personal Data Not Obtained from the Data Subject

Where the Company obtains and/or processes personal data that has not been obtained directly from the data subject, the Company ensures that the information disclosures contain in Article 14 are provided to the data subject within 30 days of our obtaining the personal data (except for advising if the personal data is a statutory or contractual requirement).

In addition to the information disclosures in section 8.1.4, where personal data has not been obtained directly from a data subject, we also provide them with information about: –

- The categories of personal data
- The source the personal data originated from and whether it came from publicly accessible sources

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication or disclosure.

Where the Company intends to further process any personal data for a purpose other than that for which it was originally obtained, we communicate this intention to the data subject prior doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the relevant section of this policy, we reserve the right not to provide the data subject with the information if: –

- They already have it and we can evidence their prior receipt of the information
- The provision of such information proves impossible and/or would involve a disproportionate effort
- Obtaining or disclosure is expressly laid down by Union or Member State law to which the Company is subject and which provides appropriate measures to protect the data subject's legitimate interest
- Where the personal data must remain confidential subject to an obligation of professional

Medtel Communications

secrecy regulated by Union or Member State law, including a statutory obligation of secrecy

7.3.1 Employee Personal Data

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

7.4 The Right of Access

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13/14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

7.4.1 Subject Access Request

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data; we provide them with: –

- The purposes of the processing
- The categories of personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- If the data has or will be disclosed to a third countries or international organizations and the appropriate safeguards pursuant to the transfer
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with a Supervisory Authority

Medtel Communications

- Where personal data has not been collected by the Company from the data subject, any available information as to the source and provider
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Subject Access Requests (SAR) are passed to the DPO as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our Information Audit to see what format it is held in, who else has it has been shared with and any specific timeframes for access.

SARs are always completed within 30-days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Please refer to our external Data subject access request procedures for the guidelines on how an SAR can be made and what steps we take to ensure that access is provided under the data protection laws.

7.5 Data Portability

The Company provides all personal information pertaining to the data subject to them on request and in a format, that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and reuse their personal data for their own purposes across different services.

To ensure that we comply with Article 20 of the data protection laws concerning data portability, we keep a commonly used and machine-readable format of personal information where the processing is based on: –

- Consent pursuant to point (a) of Article 6(1)
- Consent pursuant to point (a) of Article 9(2)
- A contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

Where requested by a data subject and if the criteria meet the above conditions, we will transmit the personal data directly from the Company to a designated controller, where technically feasible.
We utilise the below formats for the machine-readable data: –

- HTML
- CSV
- XML
- RDF
- XHTML

Medtel Communications

- PDF

All requests for information to be provided to the data subject or a designated controller are done so free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

7.6 Rectification & Erasure

7.6.1 Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d), all data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject or controller inform us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The relevant departments are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate.
Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third-party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

7.6.2 The Right to Erasure

Also, known as 'The Right to be Forgotten', the Company complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed.

All personal data obtained and processed by the Company is categorised when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

Please refer to our Data Retention Policy for exact procedures on erasing data and complying with the Article 17 requirements.

7.7 The Right to Restrict Processing

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subjects request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information

audit.

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way. The Company will apply restrictions to data processing in the following circumstances: –

- Where an individual contest the accuracy of the personal data and we are in the process verifying the accuracy of the personal data and/or making corrections
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim

The Data Protection Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third-parties. Where data is restricted, and we have disclosed such data to a third-party, we will inform the third-party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

7.8 Objections and Automated Decision Making

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection form where processing is carried out online. Individuals have the right to object to: –

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority(including profiling)
- Direct marketing (including profiling)
- Processing for purposes of scientific/historical research and statistics

Where the Company processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subjects' objection will only be considered where it is on 'grounds relating to their particular situation'. We reserve the right to continue processing such personal data where: –

- We can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual

Medtel™ Communications

- The processing is for the establishment, exercise or defense of legal claims

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

We have carried out a system audit to identify automated decision-making processes that do not involve human intervention. We also assess new systems and technologies for this same component prior to implementation. the Company understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 9 and 22 of the data protection laws, we aim to put measures into place to safeguard individuals where appropriate. Via our Privacy Notices, in our first communications with an individual and on our website, we advise individuals of their rights not to be subject to a decision when: –

- It is based on automated processing
- It produces a legal effect or a similarly significant effect on the individual

In limited circumstances, the Company will use automated decision-making processes within the guidelines of the regulations. Such instances include: –

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law(e.g. fraud or tax evasion prevention)
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where the Company uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

8 Oversight Procedures

8.1 Security & Breach Management

Alongside our 'Privacy by Design' approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security Policies provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensures that all personal data held and processed by us is accounted for and recorded, alongside risk assessments as to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has

dedicated controls and procedures in place for such situations, along with the notifications to be made to the Supervisory Authority and data subjects (where applicable).

Please refer to our Data Breach Policy & Procedures for specific protocols.

9 Transfers & Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the United States and EU are deemed less of a risk than a third country or an international organization, due to the data protection laws covering the former and the strict regulations applicable to all EU Member States.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we utilise a process that ensures such data is encrypted with a secret key and where possible is also subject to our data minimisation methods.

We use approved, secure methods of transfer and have dedicated points of contact with each Member State organization with whom we deal. All data being transferred is noted on our information audit so that tracking is easily available, and authorisation is accessible. The Data Protection Officer authorises all EU transfers and verifies the encryption and security methods and measures.

Please refer to our International Data Transfer Procedures for further details

10 Audits & Monitoring

This policy and procedure document details the extensive controls, measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls in place to protect data subjects and their information, are adequate, effective and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management Team where applicable. Data minimisation methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability. All reviews, audits and ongoing monitoring processes are recorded by the Data Protection Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: –

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance

Medtel Communications

- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

11 Training

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. Our Training & Development Policy & Procedures and Induction Policy detail how new and existing employees are trained, assessed and supported and include: –

- GDPR Workshops & Training Sessions
- Assessment Tests
- Coaching & Mentoring
- 1:1 Support Sessions
- Scripts and Reminder Aids
- Access to GDPR policies, procedures, checklists and supporting documents

Employees are continually supported and trained in the data protection laws requirements and out own objectives and obligations around data protection.

12 Penalties

The Company understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

Employees have been made aware of the severity of such penalties and their proportionate nature in accordance with the breach. We recognise that: –

- Breaches of the obligations of the controller, the processor, the certification body and the monitoring body, are subject to administrative fines up to $10,000,000 or 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- Breaches of the basic principles for processing, conditions for consent, the data subjects' rights, the transfers of personal data to a recipient in a third country or an international organization, specific processing situations (Chapter IX) or non-compliance with an order by the Supervisory Authority, are subject to administrative fines up to $20,000,000 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Medtel™ Communications

13 Responsibilities

The Company has appointed a data protection officer whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

The DPO will work in conjunction with the Compliance Officer, Marketing, Customer service managers, IT Manager and Training Officer to ensure that all processes, systems and staff are operating compliantly and within the requirements of the data protection laws and its principles.
The DPO has overall responsibility for due diligence, supporting privacy impact assessments, risk analysis and data transfers where personal data is involved and will also maintain adequate and effective records and management reports in accordance with the data protection laws and our own internal objectives and obligations.

Staff who manage and process personal or special category information will be provided with extensive data protection training and will be subject to continuous development support and mentoring to ensure that they are competent and knowledge for the role they undertake.

Medtel Communications

4.2.2.6 Vendor References
Medtel Communications – Attachment D
Business References

InfucareRX InfuCare Rx is a leading data driven nationwide specialty infusion therapy provider focused on treating patients with chronic conditions who require comprehensive clinical management services.	Chirag Shah IT Manager chirag.shah@infucarerx.com 919-518-7832 695 U.S. 46 W, Ste 100 Fairfield, NJ 07004
Allen Industries Allen Industries designs, engineers, manufactures, and installs innovative, high-quality signage across the U.S. and abroad.	John Kirschner Business Systems Manager john.kirschner@allenindustries.com 336-615-8689 4100 Sheraton Court Greensboro, NC 27410
Firkins Auto Group Firkins Auto Group, has been selling new and pre-owned vehicles in Bradenton for over 65 years.	Robbie Clemmons Director of IT rclemmons@firkins.com (941) 748-6510 2700 First St Bradenton, FL 34208
Heart Specialists of Sarasota Heart Specialists of Sarasota, FL is Sarasota's largest physician owned cardiovascular practice. Featuring a premier team of cardiologists specializing in the prevention, diagnosis, and treatment of heart and vascular conditions.	Kelly Mendoza kmendoza@heartspecialistsofsarasota.com 941-225-6006 1950 ARLINGTON STREET, SUITE 400 SARASOTA, FL 34239-3513
University of Maryland Medical Center The University of Maryland Medical Center is a teaching hospital with 806 beds based in Baltimore, Maryland, that provides the full range of health care to people throughout Maryland and the Mid-Atlantic region. It gets more than 26,000 inpatient admissions and 284,000 outpatient visits each year.	Federico Kendrick Technology Manager fkendrick@umm.edu (410) 328-9695 22 South Greene Street Baltimore, MD 21201

Medtel Communications

Medtel Communications – ATTACHMENT E
Disaster Recovery and Business Continuity

1. Business Continuity Plan
The Medtel business continuity plan (BCP) is a structured and detailed arrangement of guidelines designed to recover system and networks if they've failed or have been attacked. These plans are geared towards getting your organization operational as quickly as possible.

2. Medtel Cloud Disaster Recovery Solution
If the data center hosting your Medtel Cloud service experiences a disaster or site failure, the Medtel Cloud Disaster Recovery Solution provides continuity of service.

In normal operation, an image of your Medtel Cloud PBX is constantly updated on a remote server. When the Medtel Cloud Disaster Recovery Solution is activated, the image of your Medtel Cloud PBX is loaded onto a server in a geographically separate data center. The elastic IP address of the original Medtel Cloud PBX is pointed at the new server. Full operation is restored within minutes.

In the event of a disaster, all incoming calls to Medtel Cloud are automatically routed to the new server.

3. Continuity of Operation
Once the separate server has been created from the mirror of the data and the elastic IP address pointed at the new server, all incoming traffic again arrives at the destinations programmed in the Medtel Cloud admin portal ringing assignment. All deskphones, webphones and smartphone apps register automatically to the Medtel Cloud Disaster Recovery Solution within minutes of the switchover.

4. Recorded Calls Archive Back-Up
Archived recorded calls are stored on Medtel Cloud. Live images of the archived recordings are taken every 24 hours. Copies are maintained and backed up in accordance with agreed customer requirements.

5. Business Continuity for the Contact Center Site
In case of loss of access to the contact center site, agents may continue to work normally, from any location, using Medtel webphones on their laptops or using the Medtel smartphone apps on their cellphones.

Medtel™ Communications

4.2.2.3 Agency Support
Medtel Communications – Attachment F
Service Level Agreement

Service Level Agreement

Medtel™ Communications

Medtel Communications Service Level Agreement

Table Of Contents

1 INTRODUCTION 3
1.1 PURPOSE AND OBJECTIVES 3
1.2 PARTIES TO THE AGREEMENT 3
1.3 SUPPORT OVERVIEW 3
1.4 DEFINITION OF SERVICE AND TERMS 4
1.5 CONTACT INFORMATION 4
2 DOWNTIME RULES AND CALCULATIONS 5
2.1 DOWNTIME RULES 5
2.2 DOWNTIME CACULATIONS 5
2.3 MAXIMUM DOWNTIME CREDIT OFFERING 5
3 SERVICE DESCRIPTIONS 6
3.1 SEVERITY LEVELS 6
3.2 RESPONSE TIME 6
3.3 RESOLUTION TIME 6
4 CUSTOMER RESPONSIBILITIES 7
4.1 TROUBLE REPORTING PROCEDURES 7
4.2 ESCALATION PROCEDURES 7
5 CUSTOMER SUPPORT PROCESS 8

Medtel™ Communications

1 INTRODUCTION

1.1 PURPOSE AND OBJECTIVES

With a team of highly trained support personnel, Medtel Communications provides world class customer service and offers the following Service Level Agreement (SLA) for our customers who subscribe to our Cloud services. This SLA document has been created to clearly define the service offerings and performance levels that Medtel Communications Customer Support will deliver to its Cloud customers and Strategic Partners, as well as outlining the processes to be followed when Help Desk service is required.

1.2 PARTIES TO THE AGREEMENT

This SLA is intended to provide a structure for the support response offered to Medtel Communications cloud customers. This agreement will stand for the duration of an active subscription in good standing.

1.3 SUPPORT OVERVIEW

This SLA represents the Support team's goals and performance standards as presented below:

	Definition
Technical Support Availability	24 Hours 7 Days a Week 365 Days per Year
Average Answer time during Normal Business Hours	98% of telephony calls answered immediately. 98% of Emailed Support requests responded to within 15 minutes of receipt.
Average Answer time outside Normal Business Hours	98% of telephony calls responded to within 15 minutes. (Critical Issues Only) Email is monitored response time only applies to normal business hours.

	99.99% Uptime
Service Availability	"Unit" of Downtime = 1-60 Minutes of interrupted services. Downtime calculations begin 5 minutes after a service interruption (not defined in "Exclusions")

Medtel™ Communications

1.4 DEFINITION OF SERVICE AND TERMS

Service Availability:
"Service Availability" means the availability of cloud-based PBX voice and related functions. Medtel Communications will use commercially reasonable efforts to provide 99.99% Network and Cloud Voice Availability. "Network Availability" means the monthly uptime percentage excluding scheduled maintenance that Medtel Communications guarantees during any monthly billing cycle. "Cloud Voice Availability" means the functioning of all related cloud-based PBX services that have a direct impact on new call attempts and call completions that are guaranteed during any monthly billing cycle.

Downtime:
"Downtime" shall mean any period of time when all PBX services are unavailable or the inability to place or receive calls outside of the exclusions defined in this document.

Units of Downtime:
"Units of Downtime" are periods of service interruptions ranging from 1-60 minutes and are calculated after the first five (5) minutes of an experienced outage. Please see the Downtime Rules and Calculations section of this document for details regarding the submission for downtime unit credit.

Exclusions:
Loss of Service Availability caused by (i) issues beyond Medtel Communications' reasonable control, including, without limitation, denial of service or similar attacks, mail bombs, hardware failure, Internet availability, the customer's portion of the network, IP transit provider issues, SYN attacks or any other similar events; or (ii) any loss of Services related to periods of time where customer premises equipment, including customer provided PBX, is being replaced, repaired, or fails; or (iii) any issues related to the Services due to number porting; or (iv) system upgrades or maintenance which, when required, is typically reserved for the periods of time between 2am to 5am EST, will be excluded from Service Availability calculations.

Technical Support:
- Normal business hours Mon-Fri 8am to 8pm ET (excluding holidays)
- Any customer in good standing can Contact Customer Support for any support issue including basic moves, adds and changes
- Emergency 24X7 support is provided outside normal business hours for loss of service issues

1.5 CONTACT INFORMATION

Medtel Communications Sales and Project Management
- Corporate Office: 941-757-3484
- Email: Info@medtelcom.com
- Web Site: www.medtelcom.com

Medtel Communications Customer Support
- Customer Support Office: 1-800-404-9941
- Email: techsupport@medtelcom.com (Non-Emergency Only)

Medtel™ Communications

2 DOWNTIME RULES AND CALCULATIONS

2.1 DOWNTIME RULES

Subject to the limitations of this agreement, any time Service Availability is below Medtel's 99.99% availability goal, the customer will qualify for a credit for the downtime based on the table below up to the maximums indicated in the table. A written request for downtime credit must be made to Medtel Communications within five (5) business days after the time of the outage.

2.2 DOWNTIME CACULATIONS

Goal	Downtime	Downtime Credit
99.99% Uptime	15 to 60 minutes	1 day's credit
	61 to 120 Minutes	2 day's credit
	121 to 240 Minutes	4 day's credit
	241 to 480 Minutes	6 day's credit
	Over 480 minutes	10 day's credit

2.3 MAXIMUM DOWNTIME CREDIT OFFERING

A credit will be applied only to the month in which the outage occurred and will not exceed the maximums listed above.
Downtime calculations begin fifteen (15) minutes after an outage begins.

Medtel™ Communications

3 SERVICE DESCRIPTIONS

3.1 SEVERITY LEVELS

Severity levels are priority levels assigned to the customer's reported problem. The severity level is based upon the impact the problem has on the customer's ability to utilize services and/or conduct their business. The severity level shall be determined by the Medtel Communications Customer Support professional in cooperation with the customer or Strategic Partner.

3.2 RESPONSE TIME

The response time is the period of time that it takes the Medtel Communications Customer Support professional to address the reported problem and respond to the customer. Response time is not the same as resolution time.

3.3 RESOLUTION TIME

The resolution time is the time it takes to resolve a problem. The resolution time is different for each situation and cannot be determined until the appropriate support professional has evaluated the problem and is able to determine an approximate time to resolution.

Level	Response Time	Definition
• **Severity 1 Critical**	Less than 15 minutes	Cloud services are unavailable with significant impact to the ability to conduct business.
• **Severity 2 Major**	Less than one (1) hour	High-impact problem where call processing is continued but significantly impaired.
• **Severity 3 Minor**	Less than two (2) hours	An issue such as standard adds, moves, and changes or other problems not specifically described above.
NOTE:	Response time is established for problems reported directly to Customer Support during normal business hours M-F 8:00 AM to 8:00 PM ET	After Hours: Emergency problems reported outside normal business hours will be delivered to our On-Call Technicians. Access to this service must be made by telephone contact to the Customer Support number listed in this agreement. Email contacts are monitored outside normal business hours, but responses are made during normal business hours.

Medtel™ Communications

4 CUSTOMER RESPONSIBILITIES

The nature of Cloud services depends on the orchestration of various components that must be correctly configured and functioning. Typically, they are: the Cloud provider, the SIP trunking provider, internet access via the customer's ISP, and the local LAN connecting the various endpoints.
For example, if the customer's access to the internet is down, Medtel Communications Customer Support will give best effort to assist in identifying the problem but ultimately the Internet Service Provider (ISP) is the responsibility of the customer.

4.1 TROUBLE REPORTING PROCEDURES

Any technical trouble must be reported to the Medtel Communications Customer Support group in one of two ways:

1. **Email** to TechSupport@Medtelcom.com

- Email should be reserved for **non-critical** issues.
- Emails will be handled as a Severity 2 Level issue
- Emails are responded to during normal business hours Mon-Fri 8am to 8pm ET (excluding holidays)

2. **Call** Medtel Communications Customer Support at 1-800-444-7434

- Customer can contact Customer Support for any support issue
- Normal business hours Mon-Fri 8am to 8pm ET (excluding holidays)
- Emergency support is provided outside normal business hours

For each contact, either by Email or telephone call, a Trouble Ticket will be opened for the reported issue

- Please use the assigned ticket number for all interactions with Customer Support regarding your reported issue.
- Each issue reported will be given its own trouble ticket number to ensure proper closure for each reported problem.

4.2 ESCALATION PROCEDURES

Any Customer can ask to have an issue escalated if they feel their issue has not (or is not) being handled adequately by the Customer Support Team.
To request Escalation:

- Simply request that the reported issue be escalated.
- Any escalation will be personally addressed by the Medtel Communications VP of Operations and a response to the customer will be forthcoming.

Medtel Communications

5 CUSTOMER SUPPORT PROCESS

1. **Email Reported Issue:**	Upon receipt of an email to Medtel Communications Customer Support, our tracking system will automatically generate a trouble ticket and deliver the issue to the help desk where one of our Customer Support Team will be assigned to that ticket. The Medtel representative will contact the customer either via email or by telephone, and a severity will be assigned to the problem. **NOTE**: Email contact to Technical Support should be limited to NON-Emergency issues only.
2. **Telephony Reported Issue:**	Upon receipt of a call to Medtel Communications Customer Support, our call center contact management system will deliver the caller immediately to an idle member of our Customer Support Team who will create a trouble ticket, enter the information into our tracking system, and assign a severity to the problem. **NOTE**: Email contact to Technical Support should be limited to NON-Emergency issues only.
3. **Telephony After Hours Emergency Issue:**	When calling outside normal business hours with an emergency, your call will be addressed by our on-call technician. **NOTE**: Email contact to Technical Support should be limited to NON-Emergency issues only.
4. **Escalation:**	Any escalation request will be forwarded immediately to the VP of Operations for review and corrective action.
5. **Closing the Request or Ticket:**	All tickets will be closed after customer satisfaction has been verified by the VP of Operations.

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Proposals
Info Technology

Proc Folder: 1262796 **Doc Description:** CLOUD BASED TELEPHONY SYSTEM **Proc Type:** Central Master Agreement			**Reason for Modification:**
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2023-07-26	2023-08-10 13:30	CRFP 1500 AGO2400000001	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code:

Vendor Name: Medtel Communications

Address:

Street: 4732 E S State Road 64

City: Bradenton

State: FL Country: United States Zip: 34208

Principal Contact: Bryan Webb, CEO & President

Vendor Contact Phone: 941-751-7780 Extension:

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X **FEIN#** 84-4020734 **DATE** 08/09/2023

All offers subject to all terms and conditions contained in this solicitation

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) Bryan Webb, President & CEO

(Address) 4732 E State Road 64, Bradenton, FL 34208

(Phone Number)/ (Fax Number) 941-751-7780/941-933-1113

(Email address) bwebb@medtelcom.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code§ 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited fiAom engaging in a boycott against Israel.

Medtel Communications LLC
(Company)

(Signature of Authorized Representative)

Bryan Webb, President & CEO
(Printed Name and Title of Authorized Representative) (Date)

941-751-7780 / 941-933-1113
(Phone Number) (Fax Number)

bwebb@medtelcom.com
(Email Address)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP AGO24*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[✓]	Addendum No. 1	[ ]	Addendum No. 6
[✓]	Addendum No. 2	[ ]	Addendum No. 7
[✓]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Medtel Communications
Company

Bryan Welch
Authorized Signature

08/16/2023
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

REQUEST FOR PROPOSAL
CRRP AGO2400000001 - CLOUD BASED TELEPHONY SYSTEM

6.8. Availability of Information: Proposal submissions become public and are available for review immediately after opening pursuant to West Virginia Code §5A-3-11(h). All other information associated with the RFP, including but not limited to, technical scores and reasons for disqualification, will not be available until after the contract has been awarded pursuant to West Virginia Code of State Rules §148-1-6.3.d.

By signing below, I certify that I have reviewed this Request for Proposal in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this proposal for review and consideration; that I am authorized by the bidder to execute this bid or any documents related thereto on bidder's behalf; that I am authorized to bind the bidder in a contractual relationship; and that, to the best of my knowledge, the bidder has properly registered with any State agency that may require registration.

Medtel Communications LLC
(Company)

Bryan Webb, President & CEO
(Representative Name, Title)

941-751-7780 / 941-933-1113
(Contact Phone/Fax Number)

08/09/2023
(Date)

BETHANYWHITE

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 8/3/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER	CONTACT NAME: Bethany White	
NFP Property & Casualty Services, Inc. 141 Longwater Drive Suite 101 Norwell, MA 02061	PHONE (A/C, No, Ext): (617) 847-3900	FAX (A/C, No): (617) 847-1422
	E-MAIL ADDRESS:	
	INSURER(S) AFFORDING COVERAGE	NAIC #
	INSURER A : Federal Insurance Company	20281
INSURED	INSURER B : ACE American Insurance Company	22667
Medtel Communications LLC 2511 Corporate Way Palmetto, FL 34221	INSURER C : Endurance American Insurance Company	10641
	INSURER D :	
	INSURER E :	
	INSURER F :	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	X COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	$ 1,000,000
	CLAIMS-MADE X OCCUR			36042704-EUC	3/24/2023	3/24/2024	DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
							MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	X POLICY PRO-JECT LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
A	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	ANY AUTO						BODILY INJURY (Per person)	$
	OWNED AUTOS ONLY / SCHEDULED AUTOS			23-73597272	3/24/2023	3/24/2024	BODILY INJURY (Per accident)	$
	X HIRED AUTOS ONLY / X NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
								$
A	X UMBRELLA LIAB X OCCUR						EACH OCCURRENCE	$ 5,000,000
	EXCESS LIAB CLAIMS-MADE			7818-47-75	3/24/2023	3/24/2024	AGGREGATE	$
	DED RETENTION $						Aggregate	$ 5,000,000
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N						X PER STATUTE / OTH-ER	
	ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH)	N/A		(24) 71836317	4/22/2023	4/22/2024	E.L. EACH ACCIDENT	$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000
B	Cyber Liab/ Tech E&O			D94965585	10/3/2022	10/3/2023	Aggregate	5,000,000
C	ExcessCyber/Tech E&			PRX30011648301	10/3/2022	10/3/2023	Aggregate Limit	5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
Insurer: Chubb /Policy Number: 8263-5989 09/01/2022 - 09/01/2023
Employment Practices Liability: 3,000,000 Aggregate Limit
Crime Coverage / Employee Theft: 1,000,000 Limit

Evidence of Insurance

CERTIFICATE HOLDER

Evidence of Insurance

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Matt Thill

Medtel™
Communications

Medtel T54W

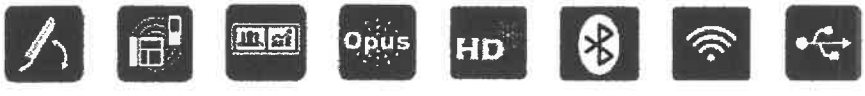
Medtel Communications

Medtel T54W

Optimum Desktop Productivity

Medtel T54W

The Medtel T54W is an easy-to-use Business Phone with an adjustable 4.3-inch color LCD screen. The Medtel T54W is a powerful and expandable office phone that delivers optimum desktop efficiency and productivity.



Adjustable Screen | Corded-Cordless Phone | Content Sharing | Opus Codec | HD Audio | Built-in Bluetooth | Built-in Wi-Fi | USB 2.0

User Friendly

Medtel T54W IP Phone features an adjustable 4.3-inch color LCD screen that you can easily adjust. The T54W is coupled with the latest version of Yealink Optimal HD Voice technologies, including Yealink Acoustic Shield technology, to eliminate background distractions and noises, delivering crystal clear voice even in a noisy environment. It also has a Hearing Aid Compatibility (HAC) handset.

Wireless Transmission

Medtel T54W has built-in Bluetooth 4.2 for Bluetooth headsets and mobile contacts synchronization. The built-in dual band Wi-Fi for Wi-Fi connectivity allows 5G Wi-Fi connectivity access.

High Expandability

With the built-in Bluetooth 4.2 and the built-in dual band 2.4G/5G Wi-Fi, the T54W offers the latest in wireless technology. Its built-in USB 2.0 port allows for USB recording or a direct wired/wireless USB headset or up to 3 EXP50 expansion modules.

Efficient Installation and Provisioning

The Medtel T54W supports efficient provisioning and effortless mass deployment. Additionally, the device is configured with a unified firmware template that applies to T53/T53W/T54W/T57W phone models for simplified management and maintenance.

Features

- 4.3" 480 x 272 pixel color display with backlight
- Adjustable LCD screen
- Dual firmware images
- Built-in Bluetooth 4.2
- Built-in dual band 2.4G/5G Wi-Fi
- USB 2.0 port
- PoE support
- HAC Handset
- Wall mountable

Medtel™
Communications

Medtel WH63

Medtel Communications

Medtel WH63

DECT Wireless Headset

The Yealink WH63 is a convertible DECT wireless headset that works seamlessly with major UC platforms and integrates natively with Yealink IP Phones. Yealink Super Wideband HD Audio Technology and Acoustic Shield Technology offer excellent audio quality for phone calls and video conferencing.

Medtel WH63

Features

- USB Connection
- Ringer on the base
- Supports busylight
- Yealink Acoustic Shield Technology
- Teams and Skype for Business compatible
- Talk Time up to 8h
- Wireless range up to 120m

Native Integration

No more EHS adapters needed, the headset connects directly to the desk phone with one USB cable. There are 2 Micro USB ports contained in the base, supporting connections with a PC and phone simultaneously.

Crystal Clear Sound

The WH63 has Yealink Acoustic Shield Technology with two built-in microphones. This automatically blocks background noise but ensures participant voices be heard clearly.

Interruption Free

Busylight is enabled in WH63, alerting others when a user is on a call, allowing users to stay focused for greater efficiency and collaboration.

Multiple Options for Comfort

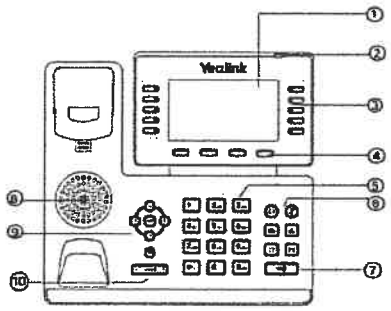
WH63 offers different accessories for comfort including: an ear-hook, headband, or neckband for personal preference. It also has a wireless range of up to 120m away from the base to allow for mobility while on a call.

Medtel™
Communications

Medtel T5 Series
Quick Reference Guide

Medtel Communications

Medtel T5 Series Soft Keys



1. LCD Screen
2. Power LED
3. Line Keys
4. Soft Keys
5. Keypad
6. Headset Key
   Mute Key
   Message Key
   Hold Key
   Redial Key
   Transfer Key
7. Speaker Phone Key
8. Speaker
9. Scroll Keys
   OK – Confirm/Answer Calls
   X – Cancel/Reject Calls
10. Volume Key

Make an Internal Call
Lift handset or press speaker button
Dial extension number
Press SEND

Make an External Call
Lift handset or press speaker button
Dial telephone number
Press SEND

Answering an Incoming Call
Incoming call notifications:

- Phone rings
- Flashing red LED light (top right)
- Incoming Caller ID is shown on the display

To answer, lift the handset or
Press the speaker button

Redial
Without lifting handset:

- Press the REDIAL button
- Use NAVIGATION KEYS to select the Contact to redial
- Press SEND
- Shortcut: Pressing the redial button twice will redial the last number called

Holding Vs. Parking a Call
Hold puts the call "On Hold" at your phone and the call can only be picked up from your phone.

Park puts the call on a "System Hold" and the parked call can be picked up from any phone on the system.

Place a Call on Hold
While on the call:
Press HOLD

Pick Up a Call from Hold
While on the call:
Press RESUME

Medtel Communications

Park a Call
While on the call:
Press an available PARK soft key
(the selected key will light up)
Hang up

Retrieve a Parked Call
Lift handset
Press the PARK soft key

Transfer a Call to Another Extension (Announced)
While on the call:

- Press TRANSFER soft key
- Dial extension number
- Press SEND
- Wait for Response & Announce Call
- Press TRANSFER soft key to complete
- Or Press END CALL then RESUME soft key to return to the call

Transfer a Call to Another Extension (Unannounced)
While on the call:

- Press TRANSFER soft key
- Dial extension Number
- Press SEND
- Press TRANSFER or hang up to complete
- Or Press END CALL to return to call

Transfer a Call Directly to Voicemail
While on the call:

- Press TRANSFER soft key
- Dial #99 + extension number and press SEND
- Press TRANSFER soft key to complete OR simply hang up.

Accessing Voicemail from Outside the Office

- Call your main office number, press # MAILBOX NUMBER
- When the company greeting answers, press * MAILBOX NUMBER
- When greeting starts, press # YOUR PIN NUMBER and follow the prompts
  Shortcuts: * + Ext = rings the phone and # + Ext = accesses voicemail

Place a Conferencing Call

- While on the 1st call, press the CONFERENCE soft key
- Dial the 2nd number (Internal or External) & press OK
- When 2nd party answers, press the CONFERENCE soft key
- All parties are connected
- If 2nd party does not answer:
  - Press the CANCEL soft key to disconnect the party
  - Press RESUME soft key to resume original call with 1st party

Activate DND (Do Not Disturb)

- Press DND soft key to send all calls directly to your voice mailbox
- Press DND soft key again to turn off DND

Medtel Communications
4732 E State Road 64 | Bradenton, FL 34208
941-751-7780 | 941-933-1133 | www.medtelcom.com

Fax

TO:	Toby L Welch	FROM:	Medtel Communications
FAX:	304-558-3970	PAGES:	2
PHONE:		DATE:	08/31/2023
RE:	CRFP AGO2400000001	CC:	

☐ Urgent ☐ For review ☐ Please comment ☐ Please reply ☐ Please recycle

VENDOR NAME: Medtel Communications LLC
BUYER: Toby L Welch
SOLICITATION NO.: CRFP AGO2400000001
BID OPENING DATE: *TECHNICAL OPENING* - Thursday August 10,2023
BID OPENING TIME: 1:30 p.m.
FAX NUMBER: 304-558-3970

To: Toby Welch

Attached is acknowledgement from Medtel Communications that we have received Addendums 1-5. Medtel Communications submitted the complete bid package on August 15, 2023.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFP AGO24*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[x]	Addendum No. 1	[ ]	Addendum No. 6
[x]	Addendum No. 2	[ ]	Addendum No. 7
[x]	Addendum No. 3	[ ]	Addendum No. 8
[x]	Addendum No. 4	[ ]	Addendum No. 9
[x]	Addendum No. 5	[ ]	Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Medtel Communications LLC
Company

Bryan Webb
Authorized Signature

08/31/2023
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012