Minimum Features of a Modern Phone System in 2025

Published March 25, 2025 40 min read

Minimum Features of a Modern Phone System in 2025

Modern enterprise phone systems have evolved far beyond basic dial-tone and voicemail. By 2025, organizations demand a rich feature set that spans ** cloud-based VoIP services, traditional PBXs, hybrid deployments, and mobile-first systems**. Whether a company operates a legacy on-premises PBX or a cutting-edge cloud communications platform, there is a baseline of functionality, security, and compliance features that **every phone system must include** to meet professional standards. This report outlines those minimum requirements – from call handling and unified communications to encryption and regulatory compliance – and explains *why each feature is essential* in today's business environment. We also compare how different system types deliver these features, providing IT managers, ** telecom engineers**, and technology strategists with a clear roadmap for evaluating phone systems in 2025.

Types of Modern Phone Systems in 2025

Modern phone systems generally fall into a few categories. Understanding their differences is key to ensuring all required features are covered:

- **Cloud-Based VoIP (UCaaS):** Cloud phone systems (often delivered as Unified Communications as a Service, UCaaS) are hosted by providers and accessed via the internet (Source: enreach.fi). They eliminate on-site hardware and offer high scalability and remote accessibility. Cloud solutions integrate voice with video conferencing, messaging, and file sharing, providing a **unified communications** experience (Source: ecn.co.za). In fact, migration to UCaaS is accelerating – by 2025, an estimated *85% of organizations will adopt a cloud-first strategy* (Source: nextiva.com). Cloud systems are favored for their fast deployment, lower upfront cost, and automatic updates (Source: aircall.io)(Source: aircall.io). They're ideal for distributed teams and can rapidly scale as the business grows (Source: aircall.io).

- ** On-Premises PBX:** A Private Branch Exchange (PBX) on-premises is a *hardware-based phone system* physically located at the business site (Source: aircall.io). Traditional PBXs (or IP-PBX for newer systems) give full control to the organization but require **significant investment and in-house IT expertise** to manage and upgrade (Source: aircall.io). They suit scenarios like a fixed office (e.g. a law firm) with stable requirements and a dedicated IT staff (Source: aircall.io). However, on-prem PBXs **struggle with remote work and rapid scaling**, and often have fewer built-in integrations with modern software (Source: aircall.io). By 2025, many enterprises are phasing out pure on-site PBXs in favor of cloud or hybrid models, except where compliance or infrastructure constraints necessitate local control.

- **Hybrid Phone Systems:** Hybrid deployments combine on-premises equipment with cloud services. For example, a company might retain an on-site PBX at headquarters but use cloud-based extensions or ** SIP trunks** to connect remote offices and mobile users. Hybrid systems aim to provide the reliability and control of on-prem hardware *plus* the flexibility of cloud. They often serve as a transitional strategy – allowing gradual migration – or as a redundancy plan (cloud failover for an on-site PBX). A well-implemented hybrid system in 2025 will still leverage cloud features (like softphone apps or analytics) while maintaining critical on-prem functions (like local trunking for sites with poor internet). **Integration and interoperability** are key: hybrid systems must seamlessly link the two environments so users experience a unified feature set.

- **Mobile-First Phone Systems:** As mobile technology dominates, some businesses adopt a **mobile-first communications** approach. A mobile-first phone system uses **smartphones as primary endpoints** and prioritizes wireless connectivity and apps over desk phones (Source: pipcall.com)(Source: pipcall.com). These systems are inherently cloud-backed – the intelligence lives in the cloud while users access services via **native mobile apps** on iOS/Android (Source: pipcall.com). They still support other devices (desktop or web clients) for versatility (Source: pipcall.com), but the design assumes employees may be on the go. In 2025, mobile-first systems are a *game-changer in organizational communication* for distributed teams (Source: pipcall.com). They deliver robust PBX features (call routing, voicemail, conferencing, etc.) through mobile interfaces (Source: pipcall.com) and leverage cellular networks (e.g. 5G) for coverage. The rise of 5G further boosts mobile-first capabilities – with broader 5G rollout in 2025, mobile users get more reliable, high-bandwidth connections to their cloud phone services (Source: ecn.co.za). This means a well-implemented mobile-centric system can offer the same quality and features as a traditional setup, with the *unparalleled flexibility* of anywhere access (Source: pipcall.com).

Each of these system types can meet modern requirements, but **only if they provide a core set of features**. The following sections detail the minimum functional, security, and compliance features that any 2025-ready phone system should include, and why they matter.

Core Functional Features Required in 2025

At a minimum, phone systems in 2025 must support a comprehensive range of **communication and call management functions**. Businesses and users have come to expect the conveniences of both traditional telephony and unified communications. Key functional features include:

- **Robust Call Handling:** Standard call control features are non-negotiable – this means call transfer, hold, call waiting, caller ID, call forwarding (including find-me/follow-me), and three-way calling. Employees should be able to seamlessly redirect calls or collaborate on calls as needed. For example, *call parking and group pickup* capabilities allow teams to handle calls flexibly across multiple devices (Source: enreach.fi). A lack of these basics can disrupt workflows and frustrate customers.

- **Voicemail and Messaging:** Modern voicemail is more than an answering machine. Systems should offer **visual voicemail** (viewing and selecting messages in an interface) and **voicemail-to-email or text transcription** for convenience (Source: enreach.fi). Unified messaging is expected: users want a single platform for voicemails, ** texts/SMS**, and possibly ** faxes** or instant messages (Source: enreach.fi)(Source: enreach.fi). Converting voice messages to text or email ensures important messages aren't missed and can be archived for records.

- **Automated Attendant and IVR:** An **auto-attendant/IVR (Interactive Voice Response)** system is considered essential for any business handling significant call volume. It greets and directs callers via menu options or voice recognition. By 2025, *62% of contact centers use IVR or voice self-service* to help route customers efficiently (Source: nextiva.com). Even smaller enterprises benefit from IVR to provide 24/7 basic service (e.g. "Press 1 for Sales") and to gather caller info upfront. Advanced IVR with natural language understanding is increasingly common, but at minimum the phone system should support DTMF menus and basic call routing rules. This reduces the workload on receptionists and **gets customers to the right department faster**, improving satisfaction (Source: aircall.io)(Source: aircall.io).

- **Intelligent Call Routing (ACD):** Beyond IVR, modern systems use **Automatic Call Distribution (ACD)** and skills-based routing to distribute calls optimally. For instance, the system might route calls based on agent skill, customer history, or time of day (Source: enreach.fi). This is critical for call centers but also for any multi-team environment – ensuring important calls reach an available team member and not languish on hold. **Intelligent call routing** improves first-call resolution and efficiency (Source: enreach.fi), making it a must-have for organizations that value customer experience.

- **Conferencing and Collaboration:** Audio conferencing (conference call bridges) is a staple, but by 2025 many phone systems also integrate **video conferencing and screen sharing** capabilities (Source: enreach.fi)(Source: enreach.fi). While video is sometimes delivered via a separate platform, a phone system should at least support multi-party audio conferences natively (so teams can set up ad-hoc conference calls). *Unified communications* features such as **team messaging, presence indication, and file sharing** are increasingly expected on the same platform (Source: smarttechfl.com)(Source: smarttechfl.com). Having these integrated (or well-integrated with external tools like Microsoft Teams) boosts collaboration – e.g. presence status shows who is available to take a call, avoiding wasted calls and voicemail tag (Source: smarttechfl.com). The emphasis on UC features is so strong that "integrating multiple channels onto one platform" is seen as *vital to productivity* in the era of remote work (Source: ecn.co.za). In short, any enterprise phone solution in 2025 should function as a **communications hub** – not just for voice, but as part of a broader collaboration ecosystem.

- **Mobility and Multi-Device Support:** With a *hybrid workforce* now the norm, phone systems must enable users to make and receive calls on any device, anywhere. This means providing **softphone apps for smartphones and desktops** with full PBX functionality (Source: pipcall.com)(Source: pipcall.com). Approximately *87% of people use a mobile phone for work communications at least once per week*, so official mobile apps are **key for secure and professional calls** (Source: nextiva.com)(Source: nextiva.com). A 2025-ready system offers features like call-pull or call flip (seamlessly moving a call between a desk phone, computer, or mobile device) without dropping the call (Source: nextiva.com). **Device-agnostic access** ensures employees remain reachable and productive whether at their desk, at home, or on the move (Source: smarttechfl.com)(Source: smarttechfl.com). Secure BYOD support is also critical – staff should be able to use personal devices with the system, under policies that protect company data (Source: smarttechfl.com). In practical terms, a minimum feature here is a *centralized user portal or app* that provides a consistent experience across mobile, desktop, and IP phone endpoints.

- **Integration with Other Systems:** In 2025, a phone system cannot exist in a silo. **Integration capabilities** – especially with CRM and customer support platforms – are considered minimum requirements for businesses that interact with customers. For example, integrating the phone system with CRM can display caller information and history to agents in real time, enabling personalized service (Source: aircall.io). This is no longer a luxury: an industry report found that *45% of communication tools in 2025 still don't integrate with CRM*, creating serious blind spots (Source: smarttechfl.com). Businesses are keen to avoid being in that 45%, so they demand integrations from their phone solutions. At the very least, modern phone systems should have **open APIs or pre-built connectors** for popular software (Salesforce, Microsoft Teams, Slack, etc.). Integration extends to click-to-dial functionality (calling out from a CRM with one click (Source: aircall.io)) and logging calls automatically to contact records. These features save time and reduce errors in dialing and data entry, directly impacting efficiency and insights.

- **Data and Analytics:** Simply handling calls is not enough; companies need to measure and improve their communication. Thus, **call analytics and reporting** tools are a baseline expectation. Even a basic system must provide call logs and usage reports. More advanced analytics (which are increasingly common) track metrics like call volumes, answer rates, average hold times, missed calls, and agent performance statistics (Source: aircall.io)(Source: aircall.io). Real-time dashboards that show active call queues or service levels are invaluable for managers and should be available in modern solutions (Source: enreach.fi)(Source: enreach.fi). Analytics help in identifying trends (e.g. peak call times) and highlight areas for training or resource adjustment. In fact, companies using analytics in their contact centers have significantly improved key metrics (e.g. using call analytics to cut average handle time by 40% in one study) (Source: nextiva.com)(Source: nextiva.com). The bottom line: any 2025 phone system aimed at enterprises **must include reporting** – and preferably real-time monitoring – to allow continuous improvement of service and resource planning.

- **High-Definition Audio & Reliability:** Users now expect landline-call quality or better over VoIP. Support for **HD voice codecs** (wideband audio such as G.722 or Opus) is a must-have feature to ensure clear voice quality on internal calls and VoIP calls (Source: enreach.fi). This improves comprehension and professionalism. Additionally, features like noise suppression (often AI-assisted) during calls are increasingly common for better call quality. Beyond audio quality, **system reliability** features are crucial: redundant call paths, failover mechanisms, and SLAs guaranteeing uptime (often 99.99% in cloud contracts) are expected by enterprise customers. A modern phone system should have *disaster recovery and redundancy* measures so that calls can continue through outages (Source: enreach.fi) (for example, automatically rerouting calls to backup lines or mobile phones if a primary system goes down). While these may be more on the architecture side, they manifest as features like backup auto-attendants or failover trunking and are absolutely essential in the feature checklist. No IT manager in 2025 will consider a phone system that cannot demonstrate high availability and resiliency.

Many systems go even further – for instance, adding **AI-powered features** (like voicemail transcription, voice assistants, or AI-based coaching for agents). These are highly valuable, but strictly speaking, AI features are emerging enhancements rather than "must-have" baseline features. However, the trend is clear: *AI is rapidly becoming ingrained* in communications. Cloud providers already offer AI voice agents to handle simple calls and AI analytics to summarize conversations (Source: aircall.io)(Source: aircall.io). Analysts predict that by 2025, **95% of customer interactions will be powered by AI** in some form (Source: nextiva.com). Thus, while an on-prem PBX might not include AI out-of-the-box, a phone system should at least *support add-ons or integrations for AI* (e.g. connecting to transcription services or chatbot frameworks) to stay future-proof.

In summary, the minimum functional portfolio of a 2025 phone system spans traditional telephony functions, **unified communications** capabilities, mobility support, and integration/analytics tools. These ensure that the phone system actively enhances productivity and customer service, rather than acting as a standalone utility. Next, we turn to the equally critical domains of security and compliance features – which have become deal-breakers in selecting any communications solution.

Security Features and Protections

Security is **not optional** in modern phone systems. With telephony integrated into IP networks and sensitive business conversations flowing through these systems, robust security features are a minimum requirement. A lapse can lead to data breaches, toll fraud losses, or regulatory penalties, so vendors and IT teams alike "build protection into their very foundation" (Source: smarttechfl.com). Key security features include:

- **End-to-End Encryption:** All voice calls, video calls, and messaging handled by the phone system should be encrypted in transit (and preferably at rest for voicemails/recordings). **End-to-end encryption** ensures that conversations cannot be intercepted or eavesdropped, which is vital for privacy (Source: smarttechfl.com). In 2025, business communications routinely involve sensitive data (customer information, confidential plans), so encryption is expected by default. For VoIP, this typically means protocols like TLS for signaling and SRTP (Secure RTP) for media. For example, cloud PBX providers in 2025 *prioritize end-to-end encryption and regular security audits* as standard practice (Source: ecn.co.za). This feature is essential not only for security but also for compliance in industries like healthcare or finance that mandate encrypted communications.

- **Secure Authentication and Access Control: Multi-factor authentication (MFA)** is a minimum requirement for administrative access and often for user access to portals or apps (Source: ecn.co.za)(Source: ecn.co.za). Relying on just passwords is too risky. MFA (e.g. a one-time code or app confirmation in addition to password) protects against unauthorized access, especially since phone system admin panels can control entire corporate communications. Alongside MFA, phone systems should offer **role-based access control**, allowing granular permission levels (so, for instance, a call center supervisor can access call recordings for their team but not system-wide settings). Audit logs of administrative actions and login attempts are another must-have for accountability and intrusion detection. This ties into the broader enterprise trend of **zero-trust security**, which phone systems should support – verifying every user and device before granting access (Source: smarttechfl.com). In practical terms, that could mean integration with single sign-on (SSO) services and device authentication certificates for SIP endpoints.

- **Network Security and Session Border Control:** If the system involves IP connectivity (which all modern ones do), it must incorporate network-layer security. **Firewalls and Session Border Controllers (SBCs)** are essential features for VoIP deployments, especially hybrid or on-premises systems. SBCs protect the voice network by inspecting and filtering SIP traffic, guarding against denial-of-service attacks and unauthorized connections. They also enable secure traversal of NAT/firewalls for remote users. In cloud phone services, the provider will include SBC functionality in their infrastructure, but enterprise IT should ensure it's there. Secure phone systems also use techniques like **rate limiting, anomaly detection, and encryption of signaling** to prevent common VoIP threats (like hijacking a SIP session or spoofing). These underlying features might not be visible to end-users but show up as capabilities like *secure remote SIP registration*, VPN support for voice, or intrusion detection alerts for suspicious call patterns.

- **Fraud Detection and Anti-Toll-Fraud Measures:** Toll fraud (hackers exploiting phone lines to make illicit international or premium-rate calls) remains a serious threat. A single PBX compromise can incur tens of thousands of dollars in charges within hours (Source: transnexus.com). In fact, some companies have been **billed millions in just days due to voice fraud attacks** (Source: itweb.co.za). Therefore, a minimum requirement is that the phone system has *fraud detection and mitigation tools*. This includes real-time monitoring of call traffic for unusual patterns (e.g. sudden spikes in international calls at odd hours) and automatic blocking or alerting if detected. Many providers now offer **call barring** options (to limit destinations or spending thresholds) and integrate with databases of known fraudulent numbers. Such features can literally save a business from catastrophic phone bills or service disruptions, as voice fraud continues to grow in sophistication.

- **Spam Call Protection and Caller ID Authentication:** Enterprises are increasingly concerned with spam and spoofed calls, which not only annoy employees but can pose security risks (vishing attacks) and harm customer trust if their number is spoofed. A modern phone system should support **STIR/SHAKEN standards** (in countries like the U.S.) for caller ID authentication, which help verify that outgoing calls from the organization are not spoofed and can be trusted. On the incoming side, systems now often include **spam call filtering** or integration with services (like spam number databases) to label or block suspected robocalls. This is important because studies show *76% of people won't even answer calls from unidentified or unfamiliar numbers* (Source: nextiva.com). Ensuring your business name/number shows correctly (via CNAM or new **Rich Caller ID** frameworks) and that your system isn't flagged as spam is crucial for effective communication. Thus, while spam prevention might involve external carrier services, the enterprise phone system should at least not be the weak link – it must pass along the proper caller identity info and enable any authentication frameworks available by 2025.

- **Compliance-Driven Security Features:** Security overlaps with compliance (discussed more below), but certain features address both. For example, **automatic call recording encryption and storage** is key if call recordings are kept (to prevent leaks of sensitive info). Another example: systems used in healthcare must have the ability to sign Business Associate Agreements and ensure HIPAA-compliant handling of data – effectively a security guarantee for PHI (protected health info). **Administrative controls** to enforce security policies (like forcing periodic password changes for voicemail or auto-logout of idle admin sessions) might seem minor, but were highlighted as one of the *"four features of secure and compliant enterprise communication"* by experts (Source: netsfere.com). In essence, a phone system must give admins the tools to implement the organization's security policies fully – this extends to **granular logging, retention settings, and integrations with security incident/event management (SIEM)** systems for centralized monitoring.

- **Secure Collaboration & Messaging:** If the phone system includes messaging (text chat) or file-sharing as part of a unified communications package, those channels need the same level of security. **End-to-end encryption for messages**, data loss prevention (DLP) controls, and the ability to remotely wipe or deactivate a lost/stolen device from the system are valuable features that professionals expect. For example, a secure mobile-first system will let an admin quickly revoke a user's app access if a phone is lost, protecting communication channels. Modern systems may also offer **secure voice/video conferencing** with features like meeting passcodes or waiting rooms to prevent unauthorized access. These collaboration security features ensure that as communications converge on the phone system platform, security scales across all media.

It's worth noting that **cloud-based phone systems often have an edge in security** for resource-constrained IT teams. A 2024 study found *94% of businesses saw improved security after switching to cloud communications*, citing benefits like built-in call encryption, 24/7 network monitoring by the provider, single sign-on support, and strong data compliance measures (Source: nextiva.com). However, on-premises systems can also be very secure if properly configured – they just require vigilant maintenance (patching, monitoring) by the enterprise. Regardless of deployment, the features above are baseline: if a phone system lacked encryption or MFA in 2025, it would be considered categorically unsafe for enterprise use ** (Source: ecn.co.za)(Source: smarttechfl.com)**.

Compliance and Regulatory Features

Phone systems in 2025 must do more than keep calls connected – they must also keep the organization on the right side of laws and industry regulations. Several compliance requirements have come into force in recent years, making certain features mandatory:

- **Emergency Calling (E911) Compliance:** Perhaps the most critical life-safety feature is compliance with emergency dialing regulations. In the U.S., **Kari's Law** and **RAY BAUM's Act** (fully effective as of 2022-2021 timelines) impose specific requirements on multi-line phone systems. Kari's Law mandates that anyone must be able to dial 911 *without any prefix* (no "9" or other digit first) and that the system automatically notifies on-site personnel (like a front desk or security) when a 911 call is made (Source: gomomentum.com). RAY BAUM's Act requires that the phone system provide a "dispatchable location" with the emergency call – meaning the caller's actual building, floor, or room location so responders know where to go (Source: gomomentum.com). **By 2025, these regulations are in full effect** for all phone systems, whether on-prem or cloud: *911 calls must be direct, instantaneous, and include precise location data* (Source: gomomentum.com). Therefore, any enterprise phone solution must include features to support this – such as configurable location information for each extension or softphone, the ability to route emergency calls to the correct 911 Public Safety Answering Point (PSAP) based on user location, and notification systems (email/SMS alerts to management when someone dials emergency). In Europe and other regions, similar **E112** and emergency caller location regulations exist, so global systems need to handle multiple emergency frameworks. Failure here is literally life-threatening and also exposes companies to legal liability and fines. A case in point: Kari's Law itself was born from a tragedy where a child could not dial 911 due to a PBX requiring a prefix (Source: gomomentum.com) – something no organization wants to ever be associated with. Thus, E911 support is absolutely a must-have feature.

- **Call Recording and Monitoring Compliance:** Many businesses record calls for training, quality assurance, or legal reasons. If call recording is used, the phone system must support compliance features around it. This includes **automated announcements or tone insertions** to notify callers of recording (as required by law in certain jurisdictions), **secure storage and retention policies** (e.g. ability to auto-delete recordings after X days to comply with privacy laws), and controlled access to recordings (only authorized roles can playback/download). For industries like finance, recordings may need tamper-evident logging and encryption to satisfy regulations. By 2025, advanced systems even use AI to help monitor compliance – for example, scanning recordings for particular keywords or to ensure agents give mandatory disclaimers (Source: enreach.fi)(Source: enreach.fi). At minimum, however, the system should allow an organization to **record calls securely and manage those records** in alignment with laws (like GDPR's right-to-be-forgotten, which might require deletion on request). Compliance also extends to **monitoring features**: if supervisors use listen-in or call-barge functions, the system should have safeguards (like whisper modes that don't violate two-party consent laws, if applicable). The inclusion of a "compliance manager" dashboard or reports can be a helpful feature to track that these controls are being followed.

- **Data Privacy and Sovereignty:** In 2025, data protection laws such as **GDPR (Europe)**, CCPA (California), POPIA (South Africa), and others are strict about personal data, which can include call logs, recordings, and even caller ID information. A modern phone system must have features or options to comply with these. For cloud services, this means offering data center locations in various regions or guarantees on data residency to keep data in-country when required. (Major UCaaS providers, for instance, let customers choose to host data in the EU to meet GDPR requirements.) It also means **compliance certifications** – a phone system provider being ISO 27001 certified or SOC 2 audited, for example, gives assurance of data handling practices. While certifications are not exactly "features", they often manifest as features like **audit trails**, **admin controls for data retention**, and **consent capture** (e.g. playing an announcement to callers in certain area codes for GDPR consent). *Built-in compliance support for data protection regulations* was highlighted as a key feature for enterprise communications (Source: smarttechfl.com). This is essential because a breach of customer call data or misuse of recordings could lead to hefty fines under laws like GDPR.

- **Industry-Specific Compliance:** Different sectors impose additional requirements. A 2025-ready phone system for healthcare should support **HIPAA compliance** – meaning it can ensure the confidentiality of patient information in communications (encryption, access control) and the vendor will sign a Business Associate Agreement. For financial services, compliance with **PCI-DSS** may be relevant if customers read credit card numbers over calls; features like DTMF tone masking (suppressing credit card digits from recordings) can help with that. Government or public-sector use might require **FedRAMP authorized** cloud services or adherence to accessibility laws (Section 508 in the U.S.). An essential feature in many cases is **comprehensive logging** – capturing call detail records, access logs, configuration changes – which can be audited by regulators or internal compliance officers. Modern phone solutions often advertise compliance modules or packages for these needs (for example, a "PCI-compliant call recording" feature). When evaluating systems, one should ensure that any domain-specific compliance features needed for their industry are either built-in or available through certified integrations.

- **Location Tracking and Mobile Compliance:** As workforces go mobile, compliance extends to mobile use as well. Some regulations now require employers to ensure even remote or mobile employees can be located when dialing emergency services (tying back to E911 requirements for softphones). Phone systems are starting to leverage **mobile device GPS or Wi-Fi positioning** to update a user's location in real-time for emergency purposes – a feature that is becoming a minimum in advanced softphone platforms by 2025. Additionally, mobile-first systems often incorporate **BYOD policy compliance**, where work calls made through the mobile app can be logged and controlled by the company (to comply with call recording rules or to ensure proper archiving if required by law, while keeping personal calls separate).

- **Telecom Regulations and Standards Compliance:** Beyond user-focused laws, a phone system must comply with telecommunications standards. For instance, by 2025 many carriers require devices or systems connecting to their network to support **IPv6** and the latest SIP standards for interoperability. Also, **numbering plan compliance** (E.164 standard for formatting phone numbers) is a basic feature to ensure international dialing works correctly. Regulatory changes like the phase-out of PSTN/ISDN in some countries (e.g. the UK's planned PSTN switch-off) mean a phone system must support SIP trunking or other IP-based trunk interfaces to future-proof connectivity. Another example is **STIR/SHAKEN** (mentioned earlier) – while largely the service provider's responsibility, a business phone system in 2025 should deliver caller ID info in a way that can be signed by carriers (e.g. not sending out invalid numbers) to comply with anti-spoofing frameworks.

- **Accessibility and Legal Requirements:** Compliance also means ensuring the phone system is usable by all employees and customers. Features supporting **accessibility** – such as TTY/TDD support for hearing-impaired users, *Real-Time Text (RTT)* for emergency calls (which is an FCC requirement for wireless carriers and increasingly for VoIP apps), adjustable volume control phones for the visually impaired, etc. – might be legally required for organizations of certain types. If the business operates contact centers, there may be requirements to use *telecommunications relay services* or provide equal access, which the phone system should not impede. While these features may not be needed by every enterprise, the system should not be inherently incompatible with accessibility tools. A compliance-minded evaluation will include these considerations, especially in government or public-facing sectors.

In essence, a phone system in 2025 needs a *compliance-by-design* approach. Providers now often bake in compliance: e.g., **in-built support for privacy legislation** like South Africa's POPIA was noted as a trend for cloud PBXs (Source: ecn.co.za). The reasoning is simple – non-compliance can result in fines, lawsuits, or business suspension. For instance, not implementing E911 properly could not only endanger lives but also result in regulatory penalties and reputational damage (Source: gomomentum.com)(Source: gomomentum.com). IT managers and tech strategists should insist on seeing how a phone system meets these compliance needs out of the box. Often, having these features ready saves considerable effort compared to custom solutions or manual processes to fill compliance gaps.

Reliability, Performance, and Management

(Beyond core features, there are some additional aspects that a modern phone system must handle, bridging functional and operational concerns. This section is included for completeness as these are often considered "table stakes" by 2025.)

- **Scalability and Flexibility:** A phone system should scale to accommodate business growth or shifting needs without major overhauls. Cloud systems excel here (allowing you to add or remove lines/users on demand) (Source: ecn.co.za), whereas on-prem PBXs should at least allow module expansions or virtualization to keep up. By 2025, even on-prem solutions often run on virtual machines or cloud-managed platforms to gain scalability. The minimum expectation is that adding a new user or a new branch office phone is a quick configuration, not a forklift hardware upgrade.

- **Performance Optimization (QoS):** Voice is real-time and sensitive to network issues. Modern systems thus come with features to ensure call quality: support for **Quality of Service (QoS) tagging**, traffic shaping, and integration with **SD-WAN** solutions are commonly expected when deploying VoIP (Source: smarttechfl.com). These features prioritize voice packets on networks and route calls optimally to minimize latency, jitter, and packet loss. For remote users, systems that adapt to low bandwidth (e.g. switching to audio-only mode or using codecs that handle poor networks) are valuable. In essence, the system must maintain voice quality across varying network conditions – a capability often highlighted by vendors offering "HD voice under any network" or mobile voice optimization.

- **Administration and User Management:** A 2025 phone system must include a **web-based management portal** that is user-friendly yet powerful. Gone are the days of programming PBXs via command-line only – IT admins expect graphical interfaces for configuring call flows, users, and policies. Moreover, **self-service user portals** are a common feature: allowing users to manage certain settings (like call forwarding, voicemail greetings, or device pairing) on their own. This reduces IT burden and is a feature many end-users appreciate. Role-based admin delegation (mentioned under security) also falls here: e.g., an office manager can be granted rights to modify hunt groups or schedules for their site without accessing global settings. The system should offer templates or batch provisioning tools if deploying at scale. In short, effective and secure *management features* are part of the minimum package – a system lacking a modern admin portal or APIs for management would feel archaic in 2025.

- **Monitoring and Alerts:** Tied to reliability, the system should provide **monitoring tools** – both in-call quality metrics (MOS scores, packet loss indicators) and system health (trunk status, bandwidth usage). Real-time alerts for issues (like if a SIP trunk goes down or if call queue times exceed a threshold) help IT staff proactively maintain service levels. Most cloud providers include a status dashboard and even proactive outage notifications. On-prem or hybrid solutions should integrate with enterprise monitoring (SNMP traps or similar). This ensures any downtime or degradation is quickly addressed, aligning with the high uptime expected.

Having discussed these essential features and characteristics, it's useful to see how the different types of phone systems compare in delivering them. The following table summarizes core features and how each system type typically addresses them:

Comparison of Core Features Across Phone System Types

FEATURE / CAPABILITY	CLOUD-BASED VOIP (UCAAS)	ON-PREMISES PBX	HYBRID SYSTEM	MOBILE-FIRST SYSTEM
Deployment & Infrastructure	Hosted by provider in cloud; minimal on-site hardware (Source: enreach.fi). Easy online management.	Hardware PBX servers on-site; requires space, power, maintenance (Source: aircall.io).	Mix of on-site PBX plus cloud services (for backup or remote users).	Cloud backend with primarily smartphone endpoints (Source: pipcall.com). Little/no on-prem hardware.
Scalability	Highly scalable on demand – add lines/users instantly via subscription (Source: aircall.io).	Limited by PBX capacity and licensing; upgrades needed for large expansions.	Scalable in each domain (add cloud users easily; on-prem part still fixed capacity).	Highly scalable (depends on cloud capacity); adding users is easy via app rollout.
Cost Model	Opex (monthly per user fees); low upfront cost (Source: aircall.io). No hardware to buy, but recurring subscription.	Capex (large upfront investment in PBX hardware and phones) (Source: aircall.io). Lower ongoing service fees (mostly trunk lines).	Mixed: upfront for on-prem portion plus subscriptions for cloud components.	Opex/subscription model; often lower cost by avoiding desk phones. Leverages users' mobile devices (BYOD).
Basic Call Features	Full suite included (voicemail, transfer, conferencing,	Full suite available if PBX modules/licenses installed. Traditional PBXs excel at basic	Should have full PBX feature set on-prem and extend select features to	Full suite offered via app (robust mobile apps ensure no feature loss) (Source: pipcall.com). May

FEATURE / CAPABILITY	CLOUD-BASED VOIP (UCAAS)	ON-PREMISES PBX	HYBRID SYSTEM	MOBILE-FIRST SYSTEM
	IVR, etc.) as part of service.	telephony features.	cloud users (depending on integration quality).	rely on cellular network for voice calls or VoIP over data.
Advanced & UC Features	Rich UC features (video meetings, team chat, presence, file sharing) often integrated into one platform (Source: ecn.co.za). AI features increasingly available (transcription, voice bots) (Source: ecn.co.za).	Basic voice features strong; advanced UC (video, chat) usually separate or add-on (e.g. separate collaboration server). Less likely to have AI unless integrated with external services.	Can offer some UC features via the cloud component (e.g. use cloud collaboration for remote users) while on-prem users may have limited UC unless hybrid integration is tight.	Focused on mobile UC: offers messaging, conferencing, etc., optimized for mobile UX. Typically integrates with collaboration apps or uses built-in smartphone capabilities.
Mobility & Remote Access	Excellent mobility – softphone apps for mobile/desktop are standard (Source: aircall.io). Users can work from anywhere with internet.	Mobility is limited: requires VPN or SBC for remote VoIP access; mobile integration possible but not inherent. Often tied to physical location.	Better than pure on-prem: cloud part handles remote users, while on-prem part covers local office. Needs good integration so remote and office users function similarly.	Mobility is core strength – designed for on-the-go use. Native mobile app is primary interface (Source: pipcall.com). Also supports desktop for flexibility (Source: pipcall.com).

FEATURE / CAPABILITY	CLOUD-BASED VOIP (UCAAS)	ON-PREMISES PBX	HYBRID SYSTEM	MOBILE-FIRST SYSTEM
Integration & APIs	Strong integration options – APIs and pre-built connectors (CRM, Teams, etc.) common. Frequent updates mean new integrations (e.g. AI CRM analytics) are available.	Integration possible via SIP or CTI, but often more limited or custom. Older PBXs may lack modern API support; newer IP-PBX can integrate but requires IT effort.	Cloud component likely provides APIs for integrations; on-prem PBX might integrate via middleware. Hybrid complexity can make seamless integration a challenge unless well-managed.	Generally offers APIs/cloud integrations similar to other cloud systems. Also often ties into mobile OS features (e.g. native dialer, contacts) for convenience.
Security Approach	Provider handles security: encryption in transit is default, data centers are secured, regular patches applied automatically (Source: ecn.co.za). Supports SSO/MFA for user logins. Certified for compliance (SOC 2, etc.).	Security is in IT's hands: can be very secure if configured (corporate firewall, SBC, encryption enabled on SIP trunks). Requires manual patching and physical security for hardware. Risk of outdated software if not maintained.	Combined: on-prem segment needs local security (firewalls, SBC), cloud segment secured by provider. Extra attention to securing the connection between on-prem and cloud (VPNs or dedicated links often used).	Heavily reliant on app/device security and cloud backend. Uses end-to-end encryption for calls and messages (Source: ecn.co.za). Mobile device management (MDM) may be needed for BYOD security. Generally inherits cloud-level security plus mobile OS security features (like biometric app lock).

FEATURE / CAPABILITY	CLOUD-BASED VOIP (UCAAS)	ON-PREMISES PBX	HYBRID SYSTEM	MOBILE-FIRST SYSTEM
Reliability & Redundancy	High redundancy – cloud providers have geo-redundant data centers, failover routing, SLAs (often 99.99%). Outages rare and resolved by provider. However, relies on internet quality at user side (mitigated by SD-WAN or 4G/5G backup).	Reliability depends on local infrastructure: can be very reliable with redundant hardware, power, and PSTN lines. But single-site PBX is a single point of failure without expensive redundancy. No external SLA – IT is responsible for uptime.	Provides redundancy if one side fails: e.g., if on-prem PBX goes down, cloud service might take over critical functions or vice versa. Hybrid can be complex but also resilient if engineered right (e.g., failover of SIP trunks to cloud).	Cloud-backend gives redundancy similar to UCaaS. If mobile data/internet fails, users can often fall back to regular cellular calls (some mobile-first systems can route calls via the PSTN cellular network as a backup). Power outages affect office less since users can operate on battery-powered devices.
Compliance Support	Vendor likely offers compliance features: E911 service with dynamic location, built-in emergency alerts; GDPR compliance with EU datacenters (Source: ecn.co.za); HIPAA-ready options, etc. Cloud systems update quickly	IT must ensure compliance: configure E911 location info for each device, implement dialing rules for Kari's Law manually, maintain call recording policies internally. Legacy systems may lack built-in tools (e.g., no automatic location tracking). Compliance achievable but	Depending on design: the cloud part can handle things like E911 for remote users, while on-prem handles local 911. Coordination needed to ensure data flows for compliance (e.g. notifications for 911 from	E911 must account for mobile nature: leading mobile-first providers use smartphone GPS/Wi-Fi to update locations or hand off to cellular 911 when appropriate. Generally will be cloud-managed for compliance similar to UCaaS. Mobile apps also need to comply with privacy (storing potentially

FEATURE / CAPABILITY	CLOUD-BASED VOIP (UCAAS)	ON-PREMISES PBX	HYBRID SYSTEM	MOBILE-FIRST SYSTEM
	to meet new regs.	requires more admin effort and third-party solutions (e.g., E911 location software).	any user). Hybrid setups must be carefully managed to not fall through cracks in compliance (ensuring both systems meet laws).	less data on device). As mobile-first is newer, most solutions are built with modern compliance (GDPR, etc.) in mind.

(Sources: characteristics synthesized from industry reports and provider documentation (Source: aircall.io)(Source: aircall.io) (Source: aircall.io)(Source: pipcall.com) (Source: ecn.co.za), as discussed in text.)

As the comparison shows, **each system type can fulfill the baseline feature requirements, but with different strengths and trade-offs**. Cloud systems excel in scalability, features, and ease of updates, whereas on-premises can be tailored and controlled at the expense of flexibility. Hybrid solutions attempt to get the best of both, though complexity is a consideration. Mobile-first systems represent a modern approach that maximizes flexibility and assumes cloud delivery. Importantly, no matter the architecture, the system must deliver on the core functional, security, and compliance features we enumerated for 2025 – otherwise it risks being outdated, insecure, or non-compliant with current business needs.

Why These Features are Essential – Expert Insights and Cases

Each feature we've listed isn't just a checkbox; it addresses real-world needs or mitigates risks that enterprises face:

- **Unified Communication & Mobility Needs:** The push for integrated voice, video, and messaging is driven by the *remote and hybrid work revolution*. As one industry analysis noted, **UCaaS is vital** because it prevents critical information from being lost across disparate tools and keeps remote teams connected seamlessly (Source: ecn.co.za). Organizations that failed to equip themselves with these capabilities struggled during the mass shift to remote work. On the mobility front, companies that stuck to legacy desk phones found themselves scrambling to forward calls to cell phones and losing oversight of communications. The stat that 87% of workers use mobile for work calls weekly (Source: nextiva.com) underscores that if your phone system doesn't properly support mobile, your employees will find their own (often insecure) workarounds. A mobile-first or at least mobile-capable system is essential to maintain productivity and security outside the office. Businesses have realized that a **flexible, device-agnostic communication system** is not just convenience, but resilience – enabling work to continue uninterrupted during office closures, travel, or any situation.

- **Security & Risk Considerations:** There are countless cautionary tales highlighting the importance of security features. For example, *voice phishing (vishing) attacks* have targeted companies by exploiting weak caller ID and authentication – leading to data breaches or financial fraud. A secure phone system that authenticates callers and implements zero-trust principles can thwart such social engineering attempts. Toll fraud incidents have literally bankrupt small businesses in the past; one FBI case in the 2010s involved criminals hacking PBXs and causing $55 million in fraudulent calls (Source: darknetdiaries.com). Today's systems come with fraud detection because these attacks continue to evolve – **an unmonitored PBX is an open bank account for hackers**. Similarly, the wave of robocalls and number spoofing in recent years (850% jump in scam calls during COVID-19 (Source: nextiva.com)) has made features like STIR/SHAKEN and spam blocking not just nice-to-have, but critical to ensure important calls get through and users don't drown in spam. We've also seen high-profile privacy scandals – for instance, if call recordings or transcripts leaked, it could violate customer privacy or insider trading laws. That's why encryption and access controls for those features are essential. As one Forbes Council expert noted, end-to-end encryption and strong administrative controls are foundational to secure enterprise communications, alongside compliance guarantees (Source: netsfere.com). The cost of a breach – whether monetary or reputational – far exceeds the cost of implementing these security measures from the start.

- **Compliance Imperatives:** The introduction of Kari's Law and RAY BAUM's Act came after tragic or critical incidents – these laws are essentially lessons written in blood and urgency. Companies have already been fined for not complying (e.g., hotels or campuses that didn't allow direct 911 dialing have faced legal and public consequences). In healthcare, regulators now pay attention to communications security – a hospital's phone system that isn't HIPAA-compliant could lead to severe penalties if investigated. Even for something as simple as not protecting credit card info over calls, businesses have been fined under PCI rules. Thus, compliance features are the *safety net and shield* for organizations: they prevent disastrous outcomes like liability for a failed 911 call, or a lawsuit for breaching customer privacy. Enterprises in 2025 often have dedicated compliance officers or consultants who will audit communication systems for these capabilities. Notably, failing to comply with E911 can even put a business's standing at risk – being non-compliant might label the business as negligent, affecting its ability to operate and contract (Source: gomomentum.com)(Source: gomomentum.com). On the positive side, having strong compliance features can be a selling point – for example, a finance firm can assure clients their calls are recorded and stored securely per regulations, building trust.

- **Expert Commentary:** Industry experts frequently emphasize that investing in modern communications is not just about convenience, but about competitiveness and risk management. Gartner's analysts have pointed out how integrated, cloud-based communications enable agility that on-prem systems struggle with – which by extension means companies with outdated systems may lag in response time and innovation. A quote from a 2025 enterprise communications report sums it up: *"Communication security isn't just nice to have—it's essential"* (Source: smarttechfl.com), highlighting that features like encryption, MFA, and compliance adherence are **non-negotiable** in vendor selection. Another telling insight from security research indicated that over 85% of businesses by 2025 are consolidating networking and security (SASE) with single providers (Source: smarttechfl.com) – signaling that companies want integrated, secure solutions rather than patchwork. This drives phone system vendors to ensure their offerings can integrate into such secure frameworks and offer all necessary protections inherently. In practical terms, experts advise creating a checklist of "non-negotiable features" when evaluating systems (Source: smarttechfl.com). These checklists invariably include the functional items (like IVR, call routing, integration) and the security/compliance ones we've discussed. The goal is to cut through marketing and ensure the chosen solution has the *substance* needed for enterprise-grade operations (Source: smarttechfl.com).

- **Case Studies:** Consider a case where a company did *not* have one of these minimum features and paid the price. One example is a mid-sized firm that experienced a PBX outage with no redundancy – they were down for nearly a day, missing customer calls and losing business. After that, they migrated to a cloud solution that guaranteed 99.99% uptime with geo-redundancy, realizing that high availability is an essential feature, not an optional extra. In another case, a financial services call center was using an outdated system without proper call encryption or controls; they suffered a breach where phone recordings of customer conversations (including personal data) were accessed by an unauthorized party. This led to regulatory investigations and a damaged reputation. The lesson learned was to implement a system with strong security and compliance certifications, and to enforce least-privilege access to sensitive data. On a more positive note, companies that embraced unified communications early were better positioned during the 2020–2021 remote work surge. Those who had a cloud

PBX with integrated video and mobile apps could transition to work-from-home in a day, whereas others scrambled to forward lines and deploy new tools. This starkly proved why features like **remote accessibility and UC integration** are essential for business continuity.

Finally, it's important to remember that **technology keeps advancing**. The "minimum" features of 2025 might become insufficient a few years later as standards rise. Thus, enterprises should look for systems that are not only compliant with today's expectations but are also **future-proof** – designed to adapt to emerging needs (be it integrating next-gen AI or meeting new security certifications). For instance, the growing use of AI in calls (for real-time language translation or sentiment analysis) could be a differentiator soon; while not mandatory in 2025, systems that allow plugging in such capabilities will serve organizations better in the long run (Source: ecn.co.za). In the same vein, with 5G and beyond, mobile-first approaches will get even more powerful, potentially making old wired phone setups obsolete. The best strategy for professionals is to ensure the phone system they choose **meets all current requirements with room to grow** – a stable, secure, feature-rich foundation on which they can build additional capabilities as needed.

Conclusion

By 2025, the benchmark for business phone systems is higher than ever. Companies expect their phone system – whether cloud, on-prem, hybrid, or mobile-centric – to deliver *complete telephony functionality, unified communications, airtight security, and rigorous compliance support* out-of-the-box. We've outlined the minimum feature set that has effectively become the entry ticket to this arena. These features are not just technical niceties; **they are driven by how modern businesses operate**, with globally distributed teams, heightened cybersecurity threats, and strict regulatory landscapes. An IT manager or telecom engineer evaluating systems in 2025 should use this feature list as a guide and a checklist. If any area is lacking (be it the ability to integrate with other tools, or the absence of end-to-end encryption, or no plan for E911), that system will likely pose a risk or cost down the line.

Fortunately, the industry trend is that even as expectations rise, solutions are becoming more accessible. Cloud providers continually update their platforms to add features (often passing new compliance mandates automatically onto customers as updates), and even traditional PBX vendors have adapted with hybrid offerings. The key is to choose a solution aligned with your organization's needs and to ensure no critical feature is missing. As we have seen, the **cost of missing features**

can be immense – from lost productivity and poor customer experience to security breaches or legal violations. Conversely, a well-chosen phone system that meets all these minimum features will serve as a resilient, flexible backbone for enterprise communications.

In summary, the minimum features a 2025 phone system must include are those that enable a business to **communicate anywhere, through any medium, securely and compliantly**. By covering modern call functionality, integrating with work tools, safeguarding every conversation, and adhering to all regulations, a phone system becomes a strategic asset rather than just an overhead. As technology strategists chart the way forward, investing in such robust communication infrastructure is essential to support business growth and stability in the digital age (Source: nextiva.com)(Source: smarttechfl.com).

Sources:

1. Enreach, *"Business phone system features checklist for 2024"* – Discussion of key features and integration considerations (Source: enreach.fi)(Source: enreach.fi).
2. Nextiva, *"40+ VoIP Statistics & Trends for 2025"* – Statistics on cloud adoption, mobile usage, AI in customer interactions, and VoIP features (Source: nextiva.com)(Source: nextiva.com).
3. SmartTech FL, *"Enterprise-Grade Communication Systems Explained (2025)"* – Insights on must-have features, security (encryption, MFA, zero-trust), SASE integration, and remote work support (Source: smarttechfl.com)(Source: smarttechfl.com).
4. ECN, *"6 Trends in Cloud PBX for 2025"* – Emphasizes UCaaS adoption, AI features, security (end-to-end encryption, MFA) and compliance with data laws (e.g. POPIA) in cloud phone systems (Source: ecn.co.za)(Source: ecn.co.za).
5. U.S. FCC / 911.gov – Kari's Law & RAY BAUM's Act requirements for multi-line telephone systems (direct 911 dialing, notification, dispatchable location) (Source: gomomentum.com)(Source: gomomentum.com).
6. ITWeb (Adapt IT), *"Voice fraud attacks cost companies millions"* – Real-world impact of PBX toll fraud and need for fraud prevention measures (Source: itweb.co.za).
7. Aircall, *"Guide to Modern Business Phone Systems in 2025"* – Breakdown of system types (on-prem, hosted PBX, etc.), and list of must-have features like call routing, IVR, CRM integration, call analytics, and AI assistants (Source: aircall.io)(Source: aircall.io).

8. Momentum Telecom, *"Guide to E911 Compliance"* – Stresses that as of 2022, all Kari's Law and RAY BAUM's Act rules are in effect and highlights consequences of non-compliance (Source: gomomentum.com)(Source: gomomentum.com).

9. Pipcall, *"Embracing Mobility: Mobile-First Phone Systems"* – Defines mobile-first systems (cloud-based core, native mobile apps, feature-rich and admin-friendly) and their benefits in flexibility and cost (Source: pipcall.com)(Source: pipcall.com).

10. Forbes Business Council (Anurag Lal), *"Four Features of Secure and Compliant Enterprise Communication"* – Identifies critical security features like end-to-end encryption, administrative controls, compliance guarantees, and cloud storage (noting what enterprises should demand for secure comms) (Source: netsfere.com).

Tags: phone systems, voip, ucaas, pbx, unified communications, telecom standards, cloud communication, enterprise telephony, security features, regulatory compliance

About ClearlyIP

ClearlyIP Inc. — Company Profile (June 2025)

1. Who they are

ClearlyIP is a privately-held unified-communications (UC) vendor headquartered in Appleton, Wisconsin, with additional offices in Canada and a globally distributed workforce. Founded in 2019 by veteran FreePBX/Asterisk contributors, the firm follows a "build-and-buy" growth strategy, combining in-house R&D with targeted acquisitions (e.g., the 2023 purchase of Voneto's EPlatform UCaaS). Its mission is to "design and develop the world's most respected VoIP brand" by delivering secure, modern, cloud-first communications that reduce cost and boost collaboration, while its vision focuses on unlocking the full potential of open-source VoIP for organisations of every size. The leadership team collectively brings more than 300 years of telecom experience.

2. Product portfolio

- **Cloud Solutions** – Including *Clearly Cloud* (flagship UCaaS), **SIP Trunking**, **SendFax.to** cloud fax, **ClusterPBX OEM**, **Business Connect** managed cloud PBX, and **EPlatform** multitenant UCaaS. These provide fully hosted voice, video, chat and collaboration with 100+ features, per-seat licensing, geo-redundant PoPs, built-in call-recording and mobile/desktop apps.

- **On-Site Phone Systems** – Including CIP PBX appliances (FreePBX pre-installed), ClusterPBX Enterprise, and Business Connect (on-prem variant). These offer local survivability for compliance-sensitive sites; appliances start at 25 extensions and scale into HA clusters.
- **IP Phones & Softphones** – Including CIP SIP Desk-phone Series (CIP-25x/27x/28x), fully white-label branding kit, and *Clearly Anywhere* softphone (iOS, Android, desktop). Features zero-touch provisioning via Cloud Device Manager or FreePBX "Clearly Devices" module; Opus, HD-voice, BLF-rich colour LCDs.
- **VoIP Gateways** – Including Analog FXS/FXO models, VoIP Fail-Over Gateway, POTS Replacement (for copper sun-set), and 2-port T1/E1 digital gateway. These bridge legacy endpoints or PSTN circuits to SIP; fail-over models keep 911 active during WAN outages.
- **Emergency Alert Systems** – Including **CodeX** room-status dashboard, **Panic Button**, and **Silent Intercom**. This K-12-focused mass-notification suite integrates with CIP PBX or third-party FreePBX for Alyssa's-Law compliance.
- **Hospitality** – Including **ComXchange** PBX plus PMS integrations, hardware & software assurance plans. Replaces aging Mitel/NEC hotel PBXs; supports guest-room phones, 911 localisation, check-in/out APIs.
- **Device & System Management** – Including **Cloud Device Manager** and **Update Control (Mirror)**. Provides multi-vendor auto-provisioning, firmware management, and secure FreePBX mirror updates.
- **XCast Suite** – Including Hosted PBX, SIP trunking, carrier/call-centre solutions, SOHO plans, and XCL mobile app. Delivers value-oriented, high-volume VoIP from ClearlyIP's carrier network.

---

3. Services

- **Telecom Consulting & Custom Development** – FreePBX/Asterisk architecture reviews, mergers & acquisitions diligence, bespoke application builds and Tier-3 support.
- **Regulatory Compliance** – E911 planning plus **Kari's Law**, **Ray Baum's Act** and **Alyssa's Law** solutions; automated dispatchable location tagging.
- **STIR/SHAKEN Certificate Management** – Signing services for Originating Service Providers, helping customers combat robocalling and maintain full attestation.
- **Attestation Lookup Tool** – Free web utility to identify a telephone number's service-provider code and SHAKEN attestation rating.
- **FreePBX® Training** – Three-day administrator boot camps (remote or on-site) covering installation, security hardening and troubleshooting.
- **Partner & OEM Programs** – Wholesale SIP trunk bundles, white-label device programs, and ClusterPBX OEM licensing.

---

4. Executive management (June 2025)

- **CEO & Co-Founder: Tony Lewis** – Former CEO of Schmooze Com (FreePBX sponsor); drives vision, acquisitions and channel network.
- **CFO & Co-Founder: Luke Duquaine** – Ex-Sangoma software engineer; oversees finance, international operations and supply-chain.
- **CTO & Co-Founder: Bryan Walters** – Long-time Asterisk contributor; leads product security and cloud architecture.
- **Chief Revenue Officer: Preston McNair** – 25+ years in channel development at Sangoma & Hargray; owns sales, marketing and partner success.
- **Chief Hospitality Strategist: Doug Schwartz** – Former 360 Networks CEO; guides hotel vertical strategy and PMS integrations.
- **Chief Business Development Officer: Bob Webb** – 30+ years telco experience (Nsight/Cellcom); cultivates ILEC/CLEC alliances for Clearly Cloud.
- **Chief Product Officer: Corey McFadden** – Founder of Voneto; architect of EPlatform UCaaS, now shapes ClearlyIP product roadmap.
- **VP Support Services: Lorne Gaetz** (appointed Jul 2024) – Former Sangoma FreePBX lead; builds 24×7 global support organisation.
- **VP Channel Sales: Tracy Liu** (appointed Jun 2024) – Channel-program veteran; expands MSP/VAR ecosystem worldwide.

---

5. Differentiators

- **Open-Source DNA:** Deep roots in the FreePBX/Asterisk community allow rapid feature releases and robust interoperability.
- **White-Label Flexibility:** Brandable phones and ClusterPBX OEM let carriers and MSPs present a fully bespoke UCaaS stack.
- **End-to-End Stack:** From hardware endpoints to cloud, gateways and compliance services, ClearlyIP owns every layer, simplifying procurement and support.
- **Education & Safety Focus:** Panic Button, CodeX and e911 tool-sets position the firm strongly in K-12 and public-sector markets.

In summary

ClearlyIP delivers a comprehensive, modular UC ecosystem—cloud, on-prem and hybrid—backed by a management team with decades of open-source telephony pedigree. Its blend of carrier-grade infrastructure, white-label flexibility and vertical-specific solutions (hospitality, education, emergencycompliance) makes it a compelling option for ITSPs, MSPs and multi-site enterprises seeking modern, secure and cost-effective communications.

DISCLAIMER

This document is provided for informational purposes only. No representations or warranties are made regarding the accuracy, completeness, or reliability of its contents. Any use of this information is at your own risk. ClearlyIP shall not be liable for any damages arising from the use of this document. This content may include material generated with assistance from artificial intelligence tools, which may contain errors or inaccuracies. Readers should verify critical information independently. All product names, trademarks, and registered trademarks mentioned are property of their respective owners and are used for identification purposes only. Use of these names does not imply endorsement. This document does not constitute professional or legal advice. For specific guidance related to your needs, please consult qualified professionals.