ChronosCodex Platform, Security, Reliability, and Ecosystem Audit

Date: 2026-06-20. Scope: Chronos CRM, MLC CRM operating proof, edge/network design, communications stack, payments, websites, domain/blog engines, and tenant security posture.

Primary systems reviewed: `/opt/chronos-crm-api`, `/opt/chronos-api`, `/opt/chronos-office-admin`, `/opt/mlc-crm`, Caddy, Cloudflared, WireGuard, systemd units, Chronos PostgreSQL database `chronoscrm`, and MLC PostgreSQL database `mlcdb`.

Important interpretation: Chronos is built from the MLC CRM operating pattern and now has a much wider SaaS/multi-tenant surface. The MLC production clone proves the core CRM/communications engine at large scale. Chronos itself is still early in tenant production data volume, so the strongest reliability claim is "proven architecture inherited from MLC, ready for controlled tenant growth," not "Chronos has already carried MLC-sized tenant traffic."

Executive verdict: Chronos is no longer just a contact database. It is a multi-tenant operating platform with CRM records, documents, forms, email, SMS, fax, phone, AI calling, website/domain provisioning, billing, wallet accounting, tenant support controls, and compliance-oriented audit paths. The platform is protected by several layers: Cloudflare, Linode/WireGuard pass-through, local Caddy routing, service hardening, PostgreSQL row-level security, explicit internal keys/tokens, and tenant feature gates.

Reliability signal: MLC CRM currently carries approximately **585,734 households**, **604,564 household members**, **600,787 household notes**, **549,485 household policies**, **2,227 communication records**, **2,156 PBX call logs**, and **4,997 PBX recordings** in the live database snapshot. That gives Chronos a meaningful proof base for the same household-centric data model and communications workflows.

Evidence Snapshot

AREA	OBSERVED STATE	AUDIT MEANING
Chronos services	`chronos-api.service` and `chronos-crm-api.service` active. Chronos CRM API runs from `/opt/chronos-crm-api/server.js`.	**Core API processes are live and supervised by systemd.**
MLC services	`mlc-crm.service`, `mlc-crm-beta.service`, `sms-gateway.service`, `ai-gateway`, `ai-voice-gateway`, Caddy, Cloudflared, WireGuard, PostgreSQL, PgBouncer, Redis, Docker, and monitoring/exporter services are active.	**The supporting ecosystem is not theoretical; it is running on the server.**
Perimeter	Cloudflared ingress exposes selected local services only, Caddy serves office UI/API locally, and WireGuard peer `wg0` had a recent handshake with steady transfer counters.	**The design avoids casually exposing every backend port to the public internet.**
Tenant isolation	Chronos RLS is enabled across many `chronos`, `crm`, and `mailbox` tables. `scripts/verify-tenant-isolation.mjs` passed 17/17 checks.	**The main cross-tenant data boundary is implemented and testable.**
Feature gating	Recent Forms gating audit confirms Forms are Agency+ at frontend route, household tab, and API middleware layers. Documents are Professional+.	**Paid features are not only hidden in the UI; sensitive routes are also gated server-side.**
Chronos tenant data volume	Database currently shows 12 agencies and 5 signups, with many tenant operational tables still empty.	**Chronos feature breadth is high, but tenant-scale production use is still early. More seeded and live tenant testing is needed before wide-open growth.**
Google Drive storage	`GOOGLE_DRIVE_CREDENTIALS_JSON` and `GOOGLE_DRIVE_ROOT_FOLDER_ID` are empty in Chronos CRM API env.	**Documents currently run in local storage mode unless Google Drive credentials are configured.**

Hosted Chronos Feature Inventory

Core CRM

- Households, clients, contacts, leads, prospects, phonebook, organizations, carriers, agents, tasks, notes, policies, commissions, payroll, renewals, DMI and age reports.
- Global search and dashboard modules for pipeline, source breakdowns, activity, effective dates, top agents, sales queues, alerts, and operational status.
- Duplicate detection and survivor-preserving merge paths exist in the backend route inventory.
- Import/export and HealthSherpa sync routes are present for enrollment-data intake and backfill.

Household Record

- Household profile is the system of record for communications, documents, forms, policies, SMS threads, call history, notes, and generated actions.
- Email, SMS, phone, fax, documents, and generated forms are intended to land back on the specific household rather than living only in external tools.
- Client record workflow supports outbound document/form email, CC, rich-text message, and auto-note history for user/action/date tracking.
- Fax transmissions can be linked to household communications and outbound fax records.

Documents and OCR

- Document Center UI and API include household documents, upload, archive/delete, download, and email endpoints.
- Current storage mode is local; Google Drive support is prepared through environment keys but not configured.
- AI vision/OCR positioning remains part of the Chronos feature set for IDs/cards and record extraction.
- Document Center is Professional+; Forms are Agency+.

Forms

- Forms Library / Form Templates is present in the UI and backend.
- Supported form families now include CMS-approved consent forms, ACORD forms prefilled from client profiles, employee/client tax forms, and Florida DCF Work Calendar.
- DCF Work Calendar is wired to household/member selection, date, case number, worked days, weekday/time shortcuts, hourly wage shortcut, signature pad, clone/edit/delete/email/fax/downloa actions, and protects the official-use-only column.
- Saved forms can be revisited and emailed through the household workflow.

Email and Inbox

- Mailbox API includes identities, threads, thread detail, send, and recipient suggestions.
- Chronos tenant plan: each paid user can receive an internal address under the Chronos domain, with household matching by client sender/recipient email.
- Inbound/outbound email should be deposited on the household communication timeline in rich text format.
- Mautic and SES-related scripts exist for email templates, sync, inbound provisioning, and domain audit.

SMS and Campaigns

- Tenant UI includes SMS Campaigns, SMS Automation, Scheduled SMS, templates, subscribers, campaign detail, logs, and cost panels.
- Campaign engines cover birthday, holidays, Mothers Day, Fathers Day, Medicare, ID-card follow-up, recurring household SMS, and manual send/schedule.
- Professional, Agency, and Brokerage are designed for simple on/off campaign toggles and per-household opt-out controls.
- SMS usage is expected to deduct from shared tenant balance across all validated phone lines and users, preventing double allowances across backup numbers.

Voice and PBX

- Chronos UI includes Phone, floating dialer, Telnyx softphone, SIP/WebRTC hooks, phone validation, assigned numbers, and usage-aware phone tabs.
- Backend includes PBX lookup/context endpoints, call logs, recordings, incoming-call lookup, voice provisioning, tenant phone numbers, and usage tracking tables.
- Independent PBX lives on a separate server path by design, giving the CRM a communications dependency that is isolated from the main web app process.
- MLC proof includes 2,156 PBX call logs and 4,997 recordings in the live DB snapshot.

Fax

- Chronos has fax routes, fax UI, event dashboard, event timeline, sheet composer, public fax media token path, and Telnyx fax webhook token path.
- The target workflow is send documents/forms by fax, capture receipt/status events, and log the outbound fax to household communications with direct link to the outbound record.
- MLC already operates two-way fax workflows and outbound records, making Chronos fax a clone-and-tenant-isolate extension rather than a new concept.

AI Assistants

- Telnyx AI Assistant integrations exist through AI gateway, AI voice gateway, Camila routes, Telnyx AI activity feeds, and lead conversion paths.
- Recent MLC Camila tuning added positive health-insurance lead behavior, CRM lead/logging tools, outbound Spanish greeting, goodbye/hangup behavior, and calmer voice cadence.
- Chronos can reuse the same assistant pattern for tenant-facing lead capture, call summaries, call outcomes, and household communication notes.

Billing, Plans, Wallets, and Payments

Stripe and Subscription Engine

- Chronos env has Stripe secret and webhook secret configured.
- Billing routes include plan, upgrade, downgrade, cancel downgrade, portal, Stripe webhook, and tenant-facing billing documents.
- Admin billing routes include wallet grant, usage rates, tier quotas, agency search, tenants, and billing insights.
- Current admin target: report active subscriptions, free-tier users, prepaid balances, credits consumed/remaining, disk allocation, SMS/minutes, and per-user breakdowns.

Wallet and Usage Accounting

- Wallet, ledger, credit buckets, monthly credits, credit expiry, usage rates, SMS cost, and voice-minute tables/scripts are present.
- Billing logic should treat tenant office usage as a shared account balance: all validated phone lines and all agents consume the same tenant allowance/credit pool.
- Outstanding test need: verify backup phone line does not grant a second minutes allowance and that multi-agent offices draw down shared credits consistently.

Websites, Domains, SEO, and Blog Engines

Public Website and Signup

- `chronoscodex.com` is a public Cloudflare Pages site backed by GitHub commits. Latest deployment previously verified successfully to production aliases `chronoscodex.com` and `www.chronoscodex.com`.
- The public site now explains the deeper CRM feature set: forms, ACORD, DCF calendar, tax forms, individualized email threads, fax records, documents/OCR, HealthSherpa sync, duplicate detection, SSN security, reports, audits, and metrics.
- The website offer now states that each purchased domain includes a free landing page, leads generated by websites go into the user's CRM leads section, and custom in-house websites are included for Agency and Brokerage.

Tenant Website Builder

- Tenant UI has a Website tab, hero image selection work, domain requests, site analytics, and admin domain request management.
- Current offer model keeps the existing wizard pricing while also supporting the in-CRM purchase flow for domain + website + hosting setup.
- Website signup captures business line, insurance categories/policy specialization, office GEO, public phone, optional toll-free number, and optional auto-blogging.
- Cloudflare account and Pages API token are present in env for backend domain/build orchestration.

Auto-Blogging and Content

- Chronos has Blog / News UI, content routes, site analytics routes, `chronos-news.service`, and `scripts/gen-chronos-news.mjs`.
- The intended add-on posts four line-of-business articles per month to improve SEO and AI-search recommendations.
- MLC has an existing auto-blogging engine that Chronos can use as the operating model, with tenant business metadata used to shape topics and language.

Domain Automation

- Chronos stores website/domain orders and agency website records in the schema, with admin tabs for domain requests.
- The strongest current state is "Cloudflare attachment and Pages deployment support exists." Full registrar purchase automation should still be treated as a controlled workflow until live purchase, DNS, SSL, Pages/custom domain, and billing reconciliation are tested end-to-end.

Security and Hardening

LAYER	IMPLEMENTED CONTROL	RELIABILITY/SECURITY VALUE
Cloudflare	Cloudflare Pages for public website; Cloudflared tunnel ingress for selected services; Cloudflare origin certs in Caddy; Cloudflare tokens configured for domain/Page operations.	Reduces public origin exposure, gives TLS/edge protection, and supports managed domain/website workflows.
Linode/WireGuard pass-through	WireGuard `wg0` link active with recent handshake and transfer counters. Design places public ingress behind Cloudflare and Linode/WireGuard path before local Caddy/services.	Creates an additional network boundary and avoids directly publishing the office server as a broad public target.
Caddy	`office.obamacarelocal.com` routes UI from dist and `/api/*` to local API; Mautic bound to local/Tailscale use; beta CRM bound to Tailscale-only HTTP; dotfiles/vendor/config/var blocked for Mautic.	Centralizes local reverse proxy rules and keeps beta/internal surfaces away from casual public routing.
Systemd	Chronos CRM API service uses hardening flags including `NoNewPrivileges`, `RestrictSUIDSGID`, `ProtectControlGroups`, `ProtectKernelTunables`, `ProtectKernelModules`, `ProtectClock`, and `PrivateTmp`.	Limits blast radius if the Node process is compromised.
Database	RLS enabled across tenant tables. Tenant isolation verifier passed 17/17. Credential columns such as password hashes/TOTP/reset tokens are denied to app role. Sessions are off-limits to `chronos_app`.	Protects tenant data boundaries even if a query path is missed at the application layer.
Authentication	TOTP/MFA components, login config, sessions, accept-invite, reset-password, and permissions APIs exist. Step-up MFA was intentionally reduced so a session validated by MFA remains valid for the session.	Balances security with usability after MFA validation. Session discipline remains important.
Internal callbacks	Internal key middleware and tokenized webhook paths exist for Stripe, Telnyx fax, SES/mail inbound, PBX, and AI callbacks.	Prevents unauthenticated external systems from casually posting into tenant records.
Feature gates	Forms Agency+, Documents Professional+, admin pages platform-admin only, and route-level mappings for many paid/admin surfaces.	Supports commercial tiering and prevents direct URL/API bypass for gated modules.
Support access	Tenant-facing support consent prompt, support access APIs, support recording/save paths, and admin impersonation flows exist.	Creates a recordable support workflow rather than silent admin access.

MLC Clone Reliability Proof

Production Data Scale

MLC TABLE/AREA	CURRENT COUNT
Households	585,734
Household members	604,564
Household notes	600,787
Household policies	549,485
Household communications	2,227
PBX call logs	2,156
PBX call recordings	4,997
Gmail match log	1,595

Communication Mix

CHANNEL / DIRECTION	COUNT
Email inbound	877
Email outbound	30
Phone inbound	315
Phone outbound	719
SMS inbound	240
SMS outbound	46

Why This Matters for Chronos

- MLC proves the household-centric model can hold hundreds of thousands of households and policy/member records on this server class.
- MLC proves live two-way communication capture across SMS, email, phone/PBX, and fax-oriented workflows.
- Chronos extends the same concept with tenant isolation, paid plans, wallet accounting, per-tenant email/phone/fax identity, and self-serve signup.
- The correct claim is that MLC validates the engine and operational pattern, while Chronos still needs tenant-scale traffic, migration, and billing-run observation.

Backend Engines and Route Surface

Chronos API dependencies: Express 5, PostgreSQL `pg`, Redis `ioredis`, AWS SES/SNS/S3/STS SDKs, Mailparser, Multer 2, PDFKit, pdf-lib, XLSX, QR code, Otplib, Anthropic SDK, CORS, and dotenv. This is a practical Node backend stack for CRM, documents/forms, mail parsing, MFA, and AI-supported workflows.

Route modules observed:

auth · dashboard · households · policies · tasks · calendar · documents · forms · fax · mailbox/gmail · sms · sms-cost · household-sms · email campaigns · email automation · automations · commissions · payroll · agents · organizations · carriers · reports · marketplace · blog/content · site analytics · billing/wallet · Stripe · admin tenants · support access · Telnyx AI · PBX internal · HealthSherpa · duplicates · notifications · logs

Current Gaps and Recommended Fixes

PRIORITY	ISSUE	RECOMMENDED FIX
P0	Chronos tenant operational data is still sparse. Many modules exist but have not yet been proven with full real tenant traffic.	Run an end-to-end tenant acceptance suite: signup, tier selection, mailbox assignment, household create, document upload, form generate, email, fax, SMS, phone validation, wallet deduction, Stripe webhook, downgrade/upgrade, export, support access, and backup/restore.
P0	Backup posture must remain visible. Prior launch audit flagged Chronos backup coverage as a blocker before broad paid launch.	Keep `chronos-tenant-backup` and database dump verification in the release checklist. Add a daily admin dashboard card showing last successful backup, restore-test age, storage location, and backup size.
P1	RLS is enabled but not forced on many tables, meaning owner/superuser paths can bypass RLS.	Audit all app DB roles. Ensure application connections use non-owner roles only. Consider `FORCE ROW LEVEL SECURITY` on tenant tables where operationally safe.
P1	Google Drive document storage is not configured, causing local-storage mode notices.	Configure `GOOGLE_DRIVE_CREDENTIALS_JSON` and `GOOGLE_DRIVE_ROOT_FOLDER_ID` or update low-tier messaging to explain local storage without exposing backend configuration names to tenants.
P1	Domain purchase automation is not yet verified as fully live from payment through registrar, DNS, Cloudflare Pages, custom domain, SSL, and CRM lead routing.	Build a staging domain purchase test harness with mock Stripe plus one real low-cost domain dry run. Log every step into domain order events.
P1	Email multi-tenant inbox assignment and household threading need live paid-user scale verification.	Create fixtures for at least two tenants with same client email shapes, send inbound/outbound replies, verify no cross-tenant leakage, and assert rich-text communication logs on the correct household.
P1	Usage accounting must prevent multiple phone lines from multiplying included minutes.	Add tests that place calls and SMS from primary/backup/agent lines under one agency and verify all usage deducts from the shared tenant wallet/allowance.
P2	Some timer-driven services are one-shot/inactive between runs, which is normal but easy to misread.	Add an operations dashboard that reports timer last-run, next-run, exit status, and log tail for monthly credits, expirations, news/blog generation, backup, transcription, and Mautic cron tasks.
P2	Secrets are stored in env files. This is operationally normal on the host, but compromise of the host can expose high-value keys.	After functional testing, rotate keys as planned. Restrict file ownership/mode, keep backups out of public paths, and consider moving highest-value secrets to a secrets manager or encrypted systemd credentials.

Bottom Line

Chronos has the depth of a real vertical SaaS platform: CRM, household timeline, documents, forms, communications, AI calls, phone/PBX, fax, billing, wallets, websites, domains, SEO/blogging, support access, compliance controls, and public signup. The underlying pattern is validated by MLC's live operational database and communications ecosystem.

The main remaining work is not inventing the product; it is proving every paid-tenant path under realistic self-serve conditions, keeping backups and usage accounting visible, and hardening integrations that can move money, send communications, or provision domains.

Source Checklist

- Service inventory: `systemctl` status checks for Chronos, MLC, SMS gateway, Cloudflared, WireGuard, Caddy, Postgres, Redis, PgBouncer, AI gateways, and scheduled jobs.
- Network/perimeter: sanitized review of `/etc/cloudflared/config.yml`, `/etc/caddy/Caddyfile`, `ip -brief addr`, and `wg show wg0`.
- Chronos data/security: direct PostgreSQL checks against `chronoscrm`, RLS table inventory, and `scripts/verify-tenant-isolation.mjs`.
- MLC scale proof: direct PostgreSQL checks against `mlcdb` for households, members, notes, policies, communications, call logs, recordings, and Gmail matching.
- Code inventory: route/module scan under `/opt/chronos-crm-api` and UI/API file scan under `/opt/chronos-office-admin/src`.
- Public website deployment: prior Cloudflare Pages verification for the latest ChronosCodex website commits and production aliases.

ChatGPT Audit Signature

Signer: ChatGPT Codex audit signer on `mlcserver`

Signature method: Ed25519 detached signature over the audit body ending at `AUDIT-SIGNED-CONTENT-END`. Verification fails if any signed audit content above this block is changed.

Signed at: `2026-06-19 21:06:14 EDT`

Signed content SHA-256: `e2edcf11a8c7d98192956c90cabbffc6be31ba2e6a8a6fe2f99b962c3de6c589`

Public key SHA-256 fingerprint:
`6037c6d2eb3a2ae6f6dbec7100376fb50f2a2aa6bcffefdc71901b050d39c577`

Detached signature, base64:
`2UvtVBOPBPdOZzgxkbZ7roypIj+o1JTgsalEtrwkARbkE5cI4dXS0AfBmvqdyFUYhY867CZ0cckD/607WMA+Dg==`

Detached signature file: `chronos-platform-ecosystem-audit-2026-06-20.signed-content.ed25519.sig`

Public key file: `chronos-platform-ecosystem-audit-2026-06-20.chatgpt-audit-public.pem`

Verification command:
```
sed '/AUDIT-SIGNED-CONTENT-END/q' src/chronos-platform-ecosystem-audit-2026-06-20.html > /tmp/chronos-audit.signed && openssl pkeyutl -verify -pubin -inkey chronos-platform-ecosystem-audit-2026-06-20.chatgpt-audit-public.pem -rawin -in /tmp/chronos-audit.signed -sigfile chronos-platform-ecosystem-audit-2026-06-20.signed-content.ed25519.sig
```

Security note: this makes the audit tamper-evident and attributable to this ChatGPT/Codex run as long as the private key stored on the server remains protected. No signature can survive compromise of the signer private key or host.