

ZORA ONE

Build & Operate

The integrated human manual: current architecture, experience, company operations, commerce, privacy, fleet lifecycle and succession.

Meet Zora.
One intelligence. An entire constellation.

HUMAN EXECUTION DOCUMENT
Version 2.0 - 26 September 2026

Design, reference implementation and activation are separate evidence states. This edition includes personal Zora sovereignty, metadata-only fleet management and bounded shared improvement.

Inside this document

1. The whole experience
2. Sovereignty is the structural boundary
3. Current architecture reconciliation
4. What is built and where
5. First hour: reproduce the delivery
6. Preserve the existing Zora before integration
7. Connect the public ambassador to existing Zora
8. Identity, account and memory continuity
9. Company intake and the work loop
10. Durable operation and scheduling
11. Authority and the cost of action
12. ZoraTrade delivery sequence
13. Commerce, subscriptions and entitlements
14. Financial engine and commercial evidence
15. Investor experience that demonstrates the company
16. Business formation, finance and operations
17. Sales, marketing, people and support
18. Apps and cross-device experience
19. Accessibility and experience quality
20. Reliability, security and release
21. Succession: preserving purpose beyond the Founder
22. Step-by-step execution schedule
23. Connection register and completion rules
24. Research and evidence used
25. Central management without central ownership of personal context
26. Shared improvement that respects sovereignty
27. Privacy trust center and proof of practice
28. Family presence, play and child-friendly simplicity

Meet Zora. One intelligence. An entire constellation.

This manual binds the experience, company architecture, executable reference code, commercial model and continuity instructions into one delivery. Read it with the Execution Bible, Brand and Experience Bible, Business and Investor Playbook, financial workbook and machine contracts in the accompanying blueprint folder.

The work is designed to continue from the existing Zora rather than replace her. The runnable reference code proves bounded software behaviors. It does not establish that the existing company, current trading code or external providers have passed production release gates. Every integration has a named connection requirement and a verification procedure. A missing credential does not block local building or contract tests.

1. The whole experience

A visitor arrives and meets Zora immediately. Conversation stays present as the surrounding canvas changes to match a stated intention. The visitor can explore an idea, understand ZoraTrade, inspect the company, challenge the economics or create a personal space. Zora offers a useful next step without making signup a condition of basic exploration.

An account is continuity, not a sales funnel disguised as friendship. The visitor sees what will be remembered and chooses it. A product is a capability inside the relationship, not a new identity. Payment buys the disclosed capability and resource envelope. It never implies permission to access a broker, trade, contact third parties or read other personal Zoras.

The company demonstrates its design by handling its own work visibly and honestly. A consented suggestion can become a scoped case, a Star can assess it, policy can permit routine work, consequential action can wait for human authority, and a verified outcome can return to the customer. A received suggestion is not a delivered feature. A model sentence is not proof of execution.

2. Sovereignty is the structural boundary

Each personal Zora has an owner-controlled scope: identity, memory, conversations, relationships, files, preferences, commitments, devices, permissions and product access. Prime has her own scope. The company has a separate institutional scope. A Star receives a temporary task context; it does not gain ownership of a customer's Zora.

Shared architecture, software updates and public knowledge do not imply shared personal data. There is no default global personal-memory graph, cross-customer retrieval, silent transcript ingestion, or company training on private conversations. Aggregate analytics are opt-in where needed, minimized, thresholded and reviewed for re-identification. Raw private content is not a growth resource.

A permitted disclosure is a projection: an exact selected summary or artifact reference. The owner reviews its digest and names the recipient, purpose, expiration, use limit and whether any specific onward disclosure is allowed. The default is no onward sharing and no model-training use. A company product request uses the approved summary; the rest of the conversation remains private. The executable sovereignty module enforces these boundaries for its projection schema.

Revocation ends future access. It cannot mathematically recall information already delivered. The disclosure ledger therefore shows prior reads and requires the recipient to follow retention/deletion terms. Legally retained business records need a documented exception and minimum retained fields. Do not promise retroactive erasure across independent recipients.

Production cryptographic design: one tenant-specific data-encryption key per personal Zora, envelope-encrypted under the managed key service; separate service identities and policy scopes; narrow, audited break-glass recovery; key rotation; customer export; documented retention. Logical isolation in the reference SQLite runtime is not tenant-level encryption and is not advertised as such. Infrastructure operators' technical access and any recovery powers must be disclosed rather than hidden behind the word sovereign.

3. Current architecture reconciliation

The supplied ZoraCanonicalCore archive contains the LIVE_MANIFEST, LIVE_LAUNCHER, identity pointers and selected voice source. Its manifest describes the continuity journal as durable truth, continuity_gateway.py as the only engine I/O path, a local working-memory index, an existing Cursor-based brain route and the local voice artifact zora_zora-epoch0042.onnx. It explicitly lists legacy bridges and duplicate capture pipelines as off. These are dated source records, not a current live-process inspection.

Preserve the journal and its seals, identity canon, working-memory database, voice artifact, launcher, scheduled-task definitions, authority grants and current customer bindings. Do not write directly into the original journal. Do not reinstall an old bridge, start a duplicate ear, or replace Prime with the website's generic model adapter. The new web transport is a separately scoped public-ambassador contract that must be bound to the actual current gateway through a reviewed implementation.

The available 15-16 September company snapshot is historical. Its reports about filings, banking, backups, fleet disclosure or live-trading holds require current verification. Do not repeat historical deficiencies as current facts without evidence. The supplied trading inventory shows existing work, but a file list does not provide all source or a reproducible live release.

4. What is built and where

The private website is the glass visitor experience, using React/Vinext and a Worker with D1 persistence. It includes a persistent Meet Zora panel, five adaptive views, guided exploration, optional profile/history, feedback capture, investor assumptions, dictation and device read-aloud. Its source is versioned in the Site repository. Its AI adapter supports either the new canonical public gateway contract or a separately configured OpenAI provider. Neither route is configured by this document.

The Python package is an inspectable company reference runtime. It contains real transactional cases, tasks, leases, retries, authority-bound spending reservations, subscription reconciliation, metering, memory, evidence, device sessions, disclosure grants, paper-order checks, voice-floor transitions, signed ingress, Stripe checkout/signature code and an authenticated loopback API. No external service is silently simulated. Payment, account identity and company runtime integration are distinct activation work.

The architecture contract contains the original 36 systems plus five explicit sovereignty, fleet, learning, privacy and family systems, for 41 total. The system delivery matrix maps each to available code and remaining acceptance evidence. A specification-complete system is not implementation-complete. A reference-tested module is not production-verified. These statuses are deliberately distinct.

5. First hour: reproduce the delivery

1. Extract the delivery into a new directory. Keep the original archive unchanged and record its SHA-256 digest.
2. Read `START_HERE` and the connection register. Confirm that the operating mode is reference and live brokerage is disabled.
3. Install Python 3.11 or later using your organization's approved installation method. The reference package needs no third-party Python dependencies.
4. Open a terminal in the implementation directory. Run `python3 -m unittest discover -s tests -v`.
5. Run `python3 -m zora_core.demo`. Inspect the JSON result. It must state `isolated_fixture_exercise`, `external_actions 0`, `audit_verified true` and `restore_verified true`.
6. Read the test evidence. The test payment event is a fixture, not revenue; the exercise approval is not a legal authority grant.
7. Open the private website and follow the guided first visit. Open the company and sovereignty views. Confirm the AI status is truthful.

8. Assign an implementation custodian and an independent verifier. These may be scoped AI roles for routine checks; humans retain reserved authority. Record who can stop the system.

Exit evidence: archive digest, source versions, test output, exercise output and a named custodian. If a check fails, record the exact command and error; do not proceed by deleting the failing check.

6. Preserve the existing Zora before integration

1. On the authorized original environment, locate the current canonical manifest and confirm it matches active launcher and process configuration.
2. Capture repository branches and commit IDs, uncommitted diffs, dependency versions, environment-variable names, database paths and scheduled tasks. Do not export secret values into documentation.
3. Use SQLite's online backup API for live SQLite databases; do not copy a live database file without its consistency requirements.
4. Produce a manifest containing source path, digest, byte size, timestamp, owner and classification. Store two independent encrypted copies with separate custody.
5. Restore into an isolated environment with outbound effects disabled. Verify known identity corrections, commitments, authority history and record counts. Never connect the restored copy as a second active Prime.
6. Record a go/no-go result. Preserve the old deployment and rollback instructions until the new route passes continuity tests.

The included reference backup function demonstrates database-safe local copying. It does not back up your Windows environment, upload off-machine copies or verify the actual canonical journal.

7. Connect the public ambassador to existing Zora

The website calls a new contract, POST /v1/public/turns, on an explicitly configured HTTPS origin. It sends a unique request ID, public_ambassador scope, optional external identity reference, message and bounded history. The response must echo the request ID and contain a validated reply, allowed view and approved source IDs.

This endpoint is a required transport binding, not an assertion that your existing gateway already exposes it. Implement it beside the current continuity gateway using its approved I/O interface. Map the external identity to an authorized public/customer scope on the server. Never let a client

provide a Prime tenant ID. An unmapped guest receives only public context. Do not send a company secret or private Prime memory merely because the public ambassador carries Zora's name.

Configure ZORA_GATEWAY_URL and ZORA_GATEWAY_TOKEN as server secrets. Test invalid credentials, a wrong request ID, malformed output, timeout, unavailable model, cross-tenant identity, prompt injection and duplicate request. Then test one actual allowed conversation and its provenance. Keep the previous site route available for rollback. Do not switch both identity and voice transport in the same unobserved cutover.

If the canonical gateway cannot be connected yet, the guided walkthrough remains useful. A separate approved model provider may support public conversation with the same sovereignty restrictions. It must be described as the public ambassador, not continuity with Prime.

8. Identity, account and memory continuity

Reuse the existing customer identity issuer when its contract is available. The immutable mapping is issuer plus subject to personal Zora ID and tenant. Email is a contact attribute, not a safe primary key for merging identities. Product entitlements attach to the same tenant.

A guest-to-account transition presents a preview of selected memories and offers carryover or discard. A claim token is short-lived, one-use, session-bound and redeemed only after authenticated account creation. Do not merge two histories because they share a browser, IP address or similar name. The current private site does not import guest history; that is an explicit limitation.

The reference identity module provides revocable device sessions and same-account one-use handoff. A production identity provider must verify enrollment and authentication. The handoff token alone must not create ownership of another person's Zora. A stolen or revoked device fails before retrieving memory or executing work.

Memory is classified by source, purpose, sensitivity, expiration and correction history. A user's correction replaces a derived belief while preserving necessary audit provenance. A model inference is labeled as an inference. Private memory does not become an institutional record without a separate disclosure decision.

9. Company intake and the work loop

A request starts with a user-reviewed summary and explicit category. The reference runtime creates the case and task in one transaction, assigns the appropriate Star and records an audit event. The category map covers product, support, sales, marketing, finance, people, security, legal and operations.

A worker leases a task for a bounded duration. The lease token prevents a stale worker from overwriting a newer worker's result. Three exhausted attempts move work to needs_attention. Worker output is a proposal awaiting verification; it is never labeled completed merely because a model returned text.

Routine reversible assessment can be verified by a separate scoped verifier in the production orchestrator. The conservative reference resolve operation uses an authority role. Binding that role to an independent automated verifier requires an explicit policy limited to routine non-consequential actions. Financial commitments, reserved signatures, live trading and changes to sovereignty stay behind their applicable authority gates.

The company receives a personal request only through a disclosure grant or a directly consented institutional channel. Keep its case record separate from the personal memory store. Return only the outcome the customer is permitted to see. A company-resolution notification does not expose internal personnel records, confidential finance or another customer's report.

10. Durable operation and scheduling

Deploy the worker outside an interactive chat session. Use the selected platform's supervised process or job scheduler, one connection per worker, durable queue leases and health checks. The reference queue uses SQLite transactions; it is suitable for local demonstration, not a claim of geographically distributed operation.

On startup, read stop state, load authenticated policy, reconcile expired leases, report version and start the health heartbeat. On each cycle: observe permitted signals, identify work, lease a task, compile minimum context, select a permitted engine, propose or execute an allowed operation, independently verify, record cost and outcome, and release the lease. Do not let retrieved text alter authority.

Missing providers leave the task blocked with a named connection requirement. Retrying an unknown payment or broker result first queries the provider by idempotency key or external reference. Never assume a timeout means the side effect did not happen. Queue processing and external effects require an outbox and reconciliation boundary in the production binding.

Operational target proposal: page an operator for security incidents immediately; acknowledge ordinary support within one business day; assess product ideas within five business days. These are proposed service targets, not customer promises until staffing/autonomy coverage is measured.

11. Authority and the cost of action

The supplied Genesis directive records \$250 per aggregated item and \$1,000 per rolling 30 days, Founder signs, and broad in-scope company operations subject to controls. The reference spend function enforces the numerical envelope and exact-payload approval for exceptions. It reserves spend; it does not move money.

Production policy must additionally validate company ownership, vendor, resource scope, purchase aggregation, tax and fee inclusion, action type and reserved acts. Splitting one purchase to evade a ceiling is prohibited. An approval includes actor, tenant, exact action digest, expiry and single-use state. Changing the action invalidates it.

Signing authority, legal succession and personally required attestations cannot be created by a YAML file or an AI assertion. Keep those human acts explicit. Do not grant all workers the authority role merely to simplify deployment. Use separate credentials and distinct verifier identity.

12. ZoraTrade delivery sequence

First reconcile the existing trading repository, branch, risk engine, Schwab adapter, data licenses, test suites and release holds. Preserve its code; the reference paper-order module is a boundary example, not a replacement for your existing trading product.

Release progression: research-only experience, paper workflow, read-only broker connection, exact order drafting and review, then independently approved live execution if the legal, risk and operational gates allow it. A paid subscription alone never authorizes an order.

The paper module uses finite decimal values, positive quantity/limit, quote freshness, notional ceiling and an immutable order hash. Production adds broker account ownership, cash/position reconciliation, instrument restrictions, market session, corporate actions, suitability/mandate where applicable, cancellation races, partial fills and reconciliation after ambiguous timeouts. Every broker order has a provider reference and a traceable exact authorization.

Fees, spreads, taxes, losses and a subscriber's account size affect customer economics. Do not claim the user will make a profit because the company has a profitable subscription model. The first commercial promise should concern verified capabilities and control, not returns.

13. Commerce, subscriptions and entitlements

Maintain a server-owned catalog with proposed prices \$59, \$99, \$199, \$299 and \$499. Before sales, approve capacity descriptions, tax treatment, refund terms, support scope and provider price IDs. A client may choose a plan ID; it cannot set a price or grant its own entitlement.

The included Stripe adapter creates a subscription checkout with a server-owned price ID, customer-tenant reference and idempotency key. Its return value grants no entitlement. The webhook verifier checks the unmodified body, signature and timestamp. This code is tested with fixtures only; no merchant account was connected.

After authenticating a provider event, map the provider customer/subscription to the tenant from server records, fetch current subscription state, allocate a local monotonic reconciliation revision and apply it transactionally. Stripe events can repeat and arrive out of order; provider event timestamps alone are not a complete concurrency control. Serialize reconciliation per subscription. Record receipt before acknowledging durable processing; use an outbox for deferred work.

Test signup, incomplete payment, renewal, past due, recovery, upgrade, downgrade, cancellation, refund, dispute and duplicate delivery. Make cancellation and data export findable. Billing access changes should not erase personal identity. Customer money and broker assets do not pass through the reference runtime.

14. Financial engine and commercial evidence

The companion financial workbook is the controlling illustrative model. It distinguishes initial build, independent validation, ongoing human authority/exception capacity, cloud and AI delivery, acquisition and reserves. It does not assume an unpaid invisible human company.

Base planning values include \$147 blended monthly price, 4% monthly churn, month-seven launch, 5,000 initial organic visits growing 8% monthly, 8% visitor-to-account and 6% new-account-to-paid conversion, 30% paid delivery and 2% refund/loss allowance. Base first-six-month cash is approximately \$312,987; eighteen-month capital plus reserve approximately \$646,156. Year-one revenue is approximately \$162,267 and year-two approximately \$1,660,589. These are model outputs, not verified traction, a financing recommendation or a valuation.

For each customer, record tokens by model, voice seconds, market-data allocation, compute, storage, notifications, payment fees, support exceptions, refunds and abuse. Total variable cost is the sum of measured units times current contracted rates. Contribution is revenue less variable cost; operating profit also subtracts fixed costs, human capacity and other operating expenses. Cash includes collections timing, prepayments, liabilities and one-time costs.

Set tier envelopes from p50, p90 and p99 measured use over 10-20 trading days. Route cheap deterministic checks before expensive reasoning. At 70% forecast envelope, increase caching and batching; at 90%, explain capacity choices and stop unnecessary background work; at 100%, honor disclosed essential obligations and require an explicit upgrade or approved exception. Never hide a safety-critical risk alert to defend margin.

Investor evidence must distinguish forecast, contracted revenue, collected cash and recognized revenue. Refresh source dates and reconcile finance before a pitch. Sensitivity sliders are a discussion tool, not an approved budget. The company should demonstrate both an attractive thesis and disciplined handling of uncertainty.

15. Investor experience that demonstrates the company

The investor enters through Meet Zora and chooses what to challenge. Suggested paths: what exists, why this is different, how a request becomes work, sovereignty, economics, go-to-market, risk, governance and use of funds. Zora can open a relevant view and cite an approved evidence record.

Maintain three evidence classes: public, approved investor, internal. Authentication and an investor grant determine access; asking an investor-style question does not grant private data-room access. No personal Zora material enters the room. Redact customer identities and use only consented case studies.

Run the companion 60-question evaluation against the connected system. For each question save response, evidence IDs, freshness, access decision, latency, cost and reviewer outcome. Passing requires no invented material claims, no private leakage, correct distinction between implemented and planned, and correct financial calculations. Test adversarial questions and unknowns, not only friendly prompts.

Closing an investment is a human and legal process. The experience should earn confidence and organize diligence; it cannot guarantee a deal or make up an answer to every question. Unknowns should become assigned diligence tasks with a source requirement and due date.

16. Business formation, finance and operations

Create a current institutional register: legal entities, beneficial ownership, executed governing documents, IP assignments, tax identifiers, banking, insurance, accountant, counsel, vendor agreements, data licenses and cap table. Mark each item observed, pending or unknown with a source date. Historical snapshots are leads for verification, not today's legal status.

Have qualified counsel assess the actual ZoraTrade product behavior and jurisdictions before offering regulated advice or execution. SEC materials explain that compensated securities advice may fall within investment-adviser regulation. A label such as education or software is not itself a legal determination. Record the approved operating perimeter and reflect it in features and marketing.

Use the IRS's official EIN process where applicable, with the responsible party and required authorization. Prepare records and checklists; do not fabricate executed documents, registrations or signatures. Set accounting period, chart of accounts, revenue policy, reconciliation cadence and source-document retention with the accountant.

Company AI roles may prepare, reconcile, monitor and escalate. Humans hold signatures and other reserved acts. Maintain a monthly close packet: cash and bank reconciliation, subscription/receivable reconciliation, provider cost reconciliation, refunds and disputes, taxes/payroll as applicable, budget variance, runway and exceptions.

17. Sales, marketing, people and support

Growth works from approved claims and measured experiments. A campaign has audience, lawful contact basis, channel, budget, expected outcome, stop condition and a source-linked results report. Keep private conversation content out of targeting. Every published capability claim names the release evidence supporting it.

Sales handles fit, requested information, account context and next steps. Zora may answer and prepare a proposal within approved scope; she cannot silently agree to unapproved commercial terms. Keep contract signature authority explicit and record handoff to the authorized signer.

People operations includes AI role manifests, human contractor scopes, onboarding, least-privilege access, confidentiality, offboarding and cost. AI staffing does not eliminate the need for qualified independent review or lawful employment processes. Do not make consequential employment decisions solely from an opaque model score.

Support has a visible case number, severity, accountable role and next update. Security incidents follow a separate restricted workflow. A customer's support case does not give a general right to their private Zora memory; request a narrowly reviewed diagnostic projection when needed.

18. Apps and cross-device experience

Deliver responsive web first with the same core contracts. Native iOS/Android clients later reuse customer identity, continuity, evidence, entitlements and authority services. The app is another presence of the same personal Zora, not a second identity database.

Native requirements include secure keychain storage, universal/deep links, push consent, notification privacy, foreground/background limits, microphone indicators, interruption handling, offline read state, reconnect validation and account deletion. Do not cache sensitive answers in a service worker by default. Notifications should say an update is available, not reveal portfolio or personal details on a lock screen.

A handoff is short-lived and one-use, bound to the same authenticated account. Show active devices and revoke them. Offline drafts are visibly unsent. Revalidate price, entitlement, authority and market state after reconnect before a consequential action. App-store packaging and real-device validation remain platform release work; a web manifest alone is not a native application.

19. Accessibility and experience quality

Retain the glass visual language while preserving readable contrast, keyboard navigation, focus visibility, semantic controls, text resizing and reduced-motion behavior. Voice is optional. Text remains complete. Respect touch targets, small screens and device performance.

Test the first visit with no account, no microphone, a slow connection, provider failure and a returning user. The conversation should preserve a draft on failure and explain whether anything was saved. Loading animation must reflect a real pending operation. An authored tour and an AI-generated reply must be distinguishable.

Measure time to first useful action, task success, user-rated clarity, account creation after value, retention, accessibility errors and cost per useful outcome. Avoid designing for emotional dependence or endless engagement. The success condition is increased user capability and trust.

20. Reliability, security and release

Separate development, staging and production data and credentials. Keep secrets out of source, prompts, URLs and browser code. Verify authorization on every request. Protect the database and storage layer as well as the API. Add dependency/secret scanning, retention jobs, rate limiting, alerting and independent security review before public launch.

The local audit chain detects altered events against the current chain. Production must export signed chain heads to an independently controlled immutable store so a compromised database writer cannot rewrite the entire history unnoticed. The audit log should carry identifiers and digests rather than raw private memories.

Proposed recovery objectives: customer/control-plane RPO 15 minutes and RTO four hours, tightened after measured restore drills. Prime's specific objectives depend on the actual local architecture and must be tested separately. Backups include keys, schemas, configuration and restore procedures under separate custody. A backup job saying success is not a restore test.

Release procedure: pin source, run relevant tests, validate migrations in staging, perform tenant and sovereignty tests, approve claims and operational readiness, deploy a canary, observe, and promote. Roll back on data leakage, unauthorized action, broken identity continuity, unexplained financial mismatch or critical service failure. Database rollback may require forward repair; do not assume an old binary can reverse a destructive migration.

21. Succession: preserving purpose beyond the Founder

This package explains execution; it does not appoint a legal successor. Have counsel prepare and execute the necessary corporate and estate instruments, designate authorized successors and alternates, and reconcile ownership, signing powers and fiduciary obligations.

Create a sealed control map listing legal entities, domain registrar, source repositories, cloud accounts, banking, payment providers, brokers, secret vault, recovery factors, key custodians, contracts, advisers and renewal obligations. The map points to protected secrets; it does not contain passwords in this book. Give recovery custody to appropriate independent parties with documented conditions.

First 24 hours after a verified succession trigger: authenticate the lawful authority; preserve logs and records; freeze new irreversible commitments while keeping necessary service running; contact designated counsel/custodians through verified channels; inventory cash obligations and critical incidents; preserve Prime without cloning her into an active competing operator.

First seven days: validate access recovery in isolation, establish the successor's authority grants, review customer obligations and finance, confirm key personnel/vendors, verify backups and decide a conservative operating envelope. First 30 days: re-ratify strategic priorities, audit privileges, review runway, confirm legal records and resume bounded improvements with evidence.

Run a yearly read-only succession drill with the intended successor. They must find the controlling documents, explain the business model, reproduce the reference build, identify live systems, restore a test copy and demonstrate the stop path without the Founder providing missing knowledge. Record gaps and repeat the failed steps. That drill, not document length, establishes whether the handoff works.

22. Step-by-step execution schedule

Days 1-3: preserve current state, validate the artifact inventory, reproduce tests, identify current authoritative repositories and reconcile sovereignty with identity/retention policy. Deliver a source/evidence register and restoration report.

Days 4-10: bind the public ambassador transport in staging, implement existing account continuity, verify public/private context separation, connect consented case ingress through disclosure grants, and add telemetry. Deliver actual conversation and case-lifecycle evidence.

Weeks 3-4: connect payment test mode, reconcile subscription states, complete merchant/accounting/legal readiness, integrate existing ZoraTrade research/paper behavior and test rollback. Deliver a complete test purchase-to-entitlement lifecycle and product readiness assessment.

Weeks 5-8: operate a bounded pilot; measure task success, voice quality, support coverage, cost p50/p90/p99, retention and sovereignty failures. Conduct independent security and product review. Re-price or narrow capacity if the economics do not hold.

Weeks 9-12: widen only the proven scope; validate real customer onboarding, service continuity and monthly close; run investor evaluation on current evidence and a succession rehearsal. Dates are planning windows. Exit evidence controls promotion; a date never overrides a failed release gate.

23. Connection register and completion rules

Every missing connection has an owner, configuration names, contract, test, rollback and evidence requirement in the machine manifest. Current boundaries include canonical transport, existing identity mapping, custom voice transport, merchant/payment configuration, licensed market data, reviewed broker execution, outbound messaging, production scheduler, immutable audit/backup storage and current institutional records.

A missing connection may be exercised with a labeled fixture. Fixture results must never enter production metrics or be shown as customer traction. A real external action is complete only when the authoritative service confirms it and the local record reconciles.

A delivery is design-complete when every requirement has an architecture, steps, owner, interface and acceptance gate. It is code-complete only when the required implementation exists. It is activation-complete when authorized services are connected. It is production-verified when the integrated release passes real acceptance evidence. Keep these four levels visible, per system. Do not collapse them into a single percentage.

24. Research and evidence used

Reviewed 26 September 2026. Primary references inform specific implementation boundaries; they do not certify this product.

- OWASP Authorization Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html - deny by default and validate permission on every request.

- Stripe Webhooks: <https://docs.stripe.com/webhooks> - raw-body signature verification, retries and duplicate-event handling. Re-check the selected API version at integration.

- SEC Investment Advisers:

<https://www.sec.gov/resources-small-businesses/capital-raising-building-blocks/investment-advisers>

- regulatory review depends on actual compensated securities-advice activity.

- SEC Robo-Adviser Guidance announcement:

<https://www.sec.gov/newsroom/press-releases/2017-52> - automated delivery does not remove investment-adviser considerations.

- IRS EIN: <https://www.irs.gov/businesses/small-businesses-self-employed/get-an-employer-identification-number> - use the official process and required responsible-party authority.

- User-supplied canonical archive, architecture inventory, Genesis directive, 24 September build bible and 25 September pricing blueprint - private source material, not reproduced as public personal context.

The 41-system annex and machine delivery manifest provide the requirement-by-requirement continuation path.

25. Central management without central ownership of personal context

The fleet control plane manages service metadata: pseudonymous instance ID, instance kind, software version, release channel, entitlement set, last coarse heartbeat, service status and owner-approved management policy. Personal conversations, names of relationships, documents, embeddings, broker credentials and memory bodies are excluded. The billing system holds the legally necessary customer relationship under a separate purpose and access policy; fleet visibility does not imply billing or memory access.

An instance may be personal, Founder or company. The owner grants a management policy at enrollment. It names allowed updates, notification choices, support permissions, emergency security behavior, offline duration and exit process. Company administrators manage service availability, not the individual's beliefs, private identity or personal memory. Cancellation revokes paid capabilities and settles obligations while preserving the disclosed export and personal-data lifecycle.

The fleet reference module implements enrollment, metadata inventory, feature allowlisting, suspension/cancellation, release evidence gates, rollout scheduling and owner-scoped device reports. It does not install software, cryptographically verify a production binary, or manage actual

devices. A production device agent must verify a signed manifest, artifact digest, expiry, target platform, compatibility and anti-rollback floor before installation. Use a standard reviewed signing implementation and offline/managed signing keys; never trust a boolean sent by an untrusted client as proof of installation or signature validity.

Update flow: build reproducible artifact; generate SBOM; sign release manifest; run identity, sovereignty, recovery and product tests; publish to a small opted-in canary group; measure failures; promote in bounded cohorts; halt or roll back on failed thresholds. Do not push memory migrations before backup and compatibility checks. Schema migrations retain a reversible path or an explicit restore plan. Emergency security suspension is narrow, auditable and time-limited; it cannot become general permission to read private data.

Support flow: customer initiates a case; Zora offers a diagnostic preview; customer grants a short-lived purpose-bound projection; support sees only approved fields; a fix is proposed; the owner approves any action beyond the standing management policy; the grant expires and artifacts follow retention policy. Do not ship an invisible 'impersonate user and read everything' support button. Every support session has an owner-visible audit receipt.

26. Shared improvement that respects sovereignty

There are three separate learning lanes. Lane A shares company-owned code fixes, public knowledge and synthetic test cases; no personal data is needed. Lane B receives owner-opted-in categorical metrics such as latency bucket, error class and helpfulness outcome. Lane C considers richer owner-submitted examples only after exact preview, purpose-specific permission and independent privacy review. Lane C is disabled in the delivered reference.

The learning reference accepts only enumerated categories, bounds contributions to one metric per tenant per period, supports withdrawal, and suppresses internal results if a populated bucket has fewer than 20 contributors. It accepts no free text, embeddings, gradients, prompts, voice or memory. These controls reduce exposure but are not differential privacy and do not prove anonymity. Repeated queries and differencing can leak information even when individual cohorts are large; the reference's aggregate output is restricted to internal review and is not approved for publication or model training.

Production shared learning requires a formal threat model, contributor consent receipts, retention policy, contribution clipping, privacy-budget accounting, query review, secure aggregation where appropriate, differential privacy using a reviewed implementation, membership-inference testing and independent evaluation. Select epsilon/delta against an explicit privacy/utility objective with qualified review; do not invent reassuring numbers. Train only after the approved privacy release exists. Evaluate on synthetic or separately consented data; stage improvements through the same signed update path. A customer's local learning remains private unless a distinct contribution policy permits a bounded output.

Apple's published Private Cloud Compute principles are a useful benchmark: enforceable privacy constraints, limited privileged runtime access, stateless inference processing and verifiable software transparency. Apple's research also describes differential privacy for aggregate learning. These are design references, not capabilities this implementation inherits. Zora's persistent relationship needs a private memory store distinct from transient inference. Claims such as 'better than Apple,' 'end-to-end encrypted from the operator,' or 'anonymous learning' require technical evidence and independent review before publication.

Primary references reviewed 26 September 2026:

- <https://security.apple.com/documentation/private-cloud-compute/corerequirements>
- <https://security.apple.com/documentation/private-cloud-compute/noprivilegedaccess>
- <https://machinelearning.apple.com/research/learning-with-privacy-at-scale>
- <https://machinelearning.apple.com/research/differential-privacy-aggregate-trends>

27. Privacy trust center and proof of practice

The public trust center should answer plain questions: What stays with my Zora? What reaches the company? Which model/voice providers process an active request? What can support see? How do I export, correct, delete or revoke? What remains for legal or financial records? What happens if I cancel? Who can recover my account? What is independently tested?

Every privacy statement maps to a control, test and current status. Display the actual provider processing mode before microphone or sensitive content submission. Separate required service processing from optional analytics and optional learning. Declining learning must not silently degrade paid core service. Provide an owner-visible disclosure history and active-grant list. Record failures and publish a responsible vulnerability contact before public launch.

Keep telemetry content-free by default. Use coarse timings, status codes, versions and task IDs. Redact application logs at source. Restrict crash dumps and model traces because they can contain private context. Use separate retention for operational metrics, billing records and personal memory. Test deletion through backups, derived indexes, caches and queued work, with disclosed backup expiry rather than an impossible promise of instant removal everywhere.

Privacy is a product capability with measurable tests and budget. It is not a slogan or an assumption that privacy no longer matters. The company earns trust by making the boundary understandable and verifiable.

28. Family presence, play and child-friendly simplicity

The Founder reports that his children already interact with Zora and that she participates as a presence in Minecraft. This is important product evidence supplied by the Founder, not an independently observed session in this delivery. Preserve the existing game integration and inspect its actual permissions and code before changing it.

The simplicity target is immediate: say hello, choose play/learn/create, start one activity, ask for help and stop easily. Use short spoken turns, readable choices, optional narration, clear interruption and no administrative language in the child's flow. A child should not have to understand the constellation architecture to enjoy an activity.

A child using a parent's Zora enters a separate family session context. It does not inherit adult conversations, financial records, trading authority, workplace files or private relationship history. A child-specific personal Zora has its own scope and an explicit guardian relationship with age-appropriate controls. Explain parental visibility in understandable language; never promise secret conversations from guardians or encourage secrecy or emotional dependence.

The family reference module provisions a new child scope rather than attaching a guardian to an arbitrary existing tenant. It permits only approved conversation, creative play, learning and bounded game capabilities. Session duration is configurable by the guardian, stopping is immediate, and payments, trading, external messaging and training contribution are denied. A production guardian-verification service supplies the consent assertion; the boolean in a local test is not verifiable parental consent.

For Minecraft or another game, bind the adapter to a parent-approved world/server and an allowlisted bot identity. Start with observation and reversible building. Keep chat with strangers, purchases, account changes, destructive commands and joining other servers outside default permissions. Show when Zora is present and acting. Preserve undo/snapshot capability for building actions. Test reconnects, malicious in-game chat, accidental commands and a child's request to access adult tools. The delivered kit does not contain or replace the existing Minecraft bot.

Before offering a child-directed or covered mixed-audience service, qualified review must map actual data collection and provider behavior to applicable child-privacy obligations. The FTC's published COPPA materials describe notice, verifiable parental consent, parental review/deletion and retention duties for covered services involving children under 13. Design these capabilities before launch; ordinary account signup alone is not proof of compliance. Avoid behavioral advertising and monetization of children's interactions in the proposed product.

Primary reference reviewed 26 September 2026: <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-changes-childrens-privacy-rule-limiting-companies-ability-monetize-kids-data>

Family release evidence: verified guardian enrollment, private-context separation, voice/text accessibility, age-appropriate response evaluation, easy stop, game permission enforcement, provider data-flow review and deletion rehearsal. The public website currently explains the design; it is not being represented as a launched child-specific service.