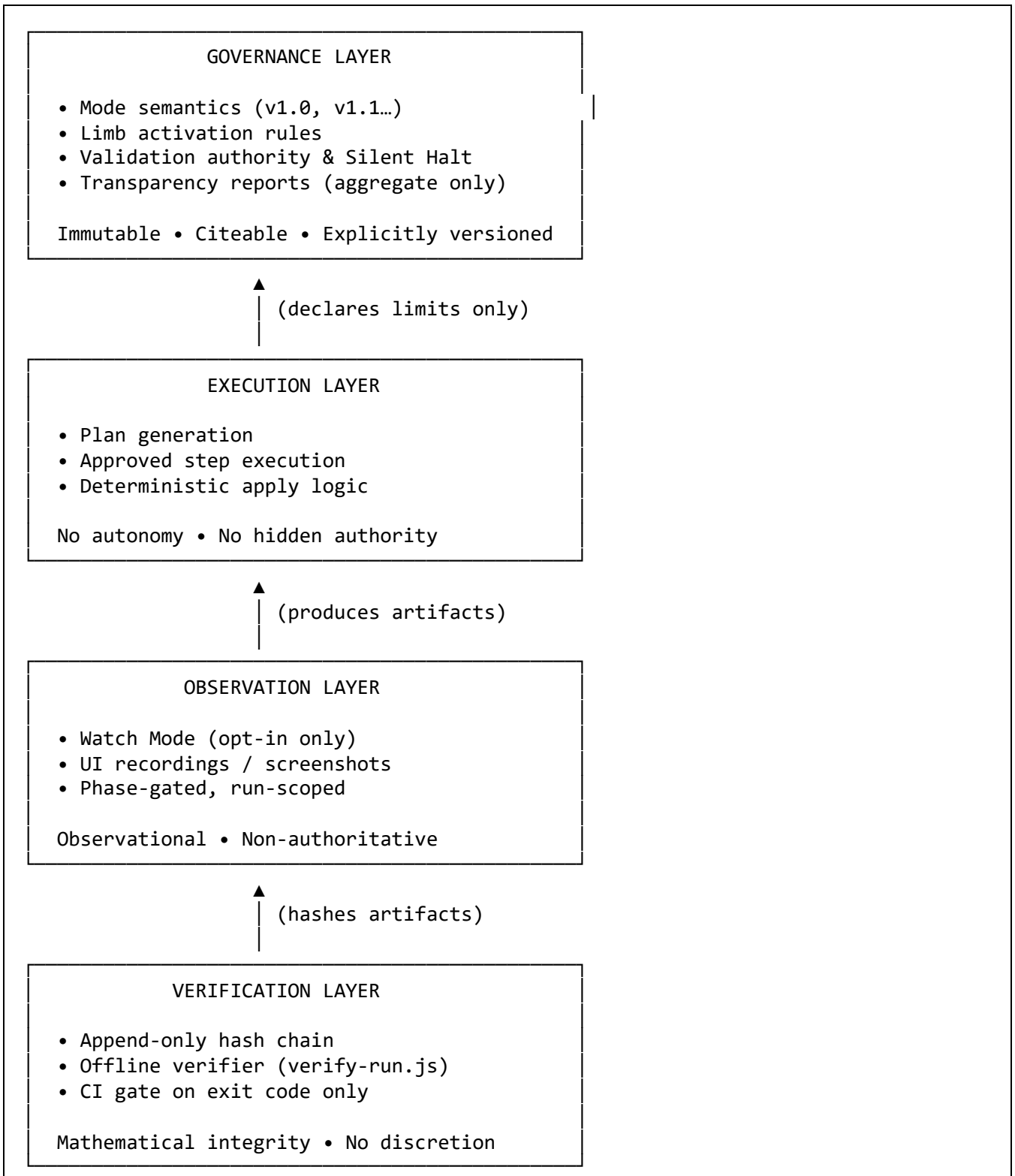
System Layers (Neutral)



Key Invariants:
• No layer can silently expand its authority
• Observation does not imply approval

- Verification proves integrity, not intent
- Governance changes require explicit versioned release

Front page: conceptual architecture only. Observation artifacts are optional and non-authoritative.

SintraPrime — Policy Appendix (Watch Mode)

Scope: non-governing transparency explanation • Format: PDF appendix (Letter, portrait)

System Integrity & Transparency Statement

> The system separates governance, execution, observation, and verification into distinct layers to prevent hidden automation or authority escalation. Execution occurs only after validation. Watch Mode, when enabled, provides phase-gated visual observation of approved actions and produces non-authoritative artifacts for transparency only. Finalized records are protected via append-only cryptographic hashing and can be verified independently using an offline tool. Governance behavior is versioned and immutable absent explicit release. This architecture enables transparency and auditability without introducing autonomous control.

Pinned clause families (by platform)

Mapping to common policy clause families; no clause numbers (they change by revision).

This section anchors Watch Mode posture to publicly verifiable policy texts.
• It includes stable URLs and small verbatim excerpts.
• It avoids "clause numbers" where policies are not numbered or may be renumbered.
• Accessed: 2026-01-12

Pinned mapping — TikTok
• Source: TikTok Developer Terms of Service (Last modified: Dec 26, 2025)
- <https://www.tiktok.com/legal/page/global/tik-tok-developer-terms-of-service/en>
• Verbatim anchors (selected):
- "use automated means in your Application to collect information from or otherwise interact with the TikTok Developer Services"
- "exceeds reasonable request volume, constitutes excessive or abusive usage"
- "bypass, circumvent or attempt to bypass or circumvent any measures we may use to prevent or restrict access"
- "build, help build, or supplement any profiles, databases, or similar records"
• Watch Mode posture mapping:
- Automation & platform integrity: Watch Mode does not post, message, or engage; it is observational only.
- Scraping / data access: Watch Mode does not crawl or bulk-extract; it captures human-equivalent visual context.
- Circumvention / evasion: Watch Mode does not bypass access controls or technical limitations.

Pinned mapping — Google
• Source: Google APIs Terms of Service (Last modified: Nov 9, 2021)
- <https://developers.google.com/terms>
• Verbatim anchors (selected):
- "You will only access (or attempt to access) an API by the means described in the documentation of that API."
- "You agree to, and will not attempt to circumvent, such limitations documented with each API."

- “Scrape, build databases, or otherwise create permanent copies of such content”
• Watch Mode posture mapping:
- Permitted access: Watch Mode does not create alternate access paths; it records visual context only.
- API limitations / circumvention: Watch Mode does not circumvent limits.
- Content handling: Watch Mode is not a scraping or database-building mechanism.

Pinned mapping — Meta
• Source: Meta Platform Terms
- <https://developers.facebook.com/terms/>
• Verbatim anchors (selected):
- “You must also comply with the applicable requirements in our Developer Policies and those made available on our Developer Site, including in our Documentation”
- “Attempting to decode, circumvent, re-identify, de-anonymize, unscramble, unencrypt, or reverse hash”
- “Processing Platform Data for purposes other than the applicable permitted purposes set forth in Meta’s Developer Docs.”
• Watch Mode posture mapping:
- Integrity & anti-circumvention: Watch Mode does not decode/circumvent protections.
- Purpose limitation: Watch Mode is observational and does not expand data processing scope.

Pinned mapping — Stripe
• Source: Stripe Services Agreement—General Terms (Last modified: Nov 18, 2025)
- <https://stripe.com/legal/ssa>
• Verbatim anchors (selected):
- “User must use the Services solely for User’s Business Purposes and in compliance with the Documentation.”
- “circumvent any technical limitations of the Services”
- “access or attempt to access non-public Stripe systems or data”
• Watch Mode posture mapping:
- Controls: Watch Mode does not initiate or alter transactions; it records contextual screenshots only.
- Anti-circumvention: Watch Mode does not bypass technical limitations or access non-public systems.

Pinned mapping — GitHub
• Source: GitHub Acceptable Use Policies
- <https://docs.github.com/en/site-policy/acceptable-use-policies/github-acceptable-use-policies>
• Verbatim anchors (selected):
- “automated excessive bulk activity and coordinated inauthentic activity”
- “Scraping refers to extracting information from our Service via an automated process”
- “You may not use information from the Service (whether scraped, collected through our API, or obtained otherwise) for spamming purposes”
• Watch Mode posture mapping:
- Automation / scraping: Watch Mode is not a scraper and does not perform bulk automated activity.

- Writes & execution: Watch Mode does not modify repos; it records contextual artifacts only.
- Integrity: offline verification checks artifact integrity; it does not confer authorization.

Alignment Notes (Common Policy Clause Families)

These notes are phrased to map to common reviews of automation, scraping/data-access, and integrity/anti-circumvention.

Automation / non-autonomy
• Watch Mode is observational only and does not initiate actions.
• Execution is approval-gated; Watch Mode does not approve, modify, or expand scope.

Scraping and data access
• Watch Mode does not crawl, scrape, or bulk-extract.
• It records human-equivalent visual context within authenticated sessions.

Integrity / anti-circumvention
• Artifacts are run-scoped evidence outputs.
• Integrity can be checked via append-only hashing and offline verification.
• Verification is deterministic and non-governing.

Platform-Specific Explanations (Copy/Paste)

TikTok
> **Transparency & Safety Context.**
> SintraPrime includes an optional Watch Mode that provides visual observability of approved actions without enabling automated posting, interaction, or decision-making. Watch Mode records only what a human operator would see during limited, opt-in phases and does not initiate, modify, or amplify content. All artifacts are run-scoped, non-authoritative, and independently verifiable. This design supports transparency and review while avoiding autonomous behavior or engagement manipulation.

Google
> **Auditability & Control Overview.**
> SintraPrime's Watch Mode enables supervised observation of validated actions without granting execution authority or adaptive autonomy. Observation is phase-gated, opt-in, and limited to visual capture of authenticated interfaces. Generated artifacts are isolated per run and cryptographically verifiable offline. This separation of observation from execution aligns with control, auditability, and safety expectations for automated systems.

Meta
> **Integrity & Oversight Statement.**
> SintraPrime implements Watch Mode as a transparency feature that allows human-supervised visual observation of approved actions without enabling automated decision-making or content interaction. Watch Mode does not post, message, or engage; it produces contextual artifacts only.

Integrity is ensured through append-only hashing and independent verification, supporting oversight without introducing autonomous behavior.

Stripe
> **Risk & Control Summary.**
> SintraPrime's Watch Mode is a non-authoritative observability feature designed to improve audit clarity without increasing operational risk. It records visual context of pre-approved actions during specified phases and cannot initiate or alter transactions. All outputs are run-scoped and hash-verified, supporting internal controls and independent review without introducing autonomous execution.

GitHub
> **Operational Transparency Note.**
> SintraPrime provides Watch Mode to enable phase-gated visual observation of approved operations without granting write access or autonomous control. Watch Mode does not execute code or modify repositories; it produces contextual artifacts only. Artifacts are run-scoped and verifiable offline, supporting reproducibility and review without impacting execution semantics.

Note: Watch Mode is observational only. Verification is deterministic and offline. This appendix does not confer authority or change system behavior.