

GOVERNED AI INFRASTRUCTURE

VerityOS Pilot & Deployment Guide

For public-sector and regulated institutions

Institutional knowledge.
Human authority.
Verifiable execution.

Verity Record

Verity Record

Export organization evidence

Integrity verification confirms that recorded evidence has not changed. Provenance shows the recorded path that produced the result. Neither proves factual truth. Do not read these labels as Fact Verified or Truth Verified.

● INTEGRITY VERIFIED

● PROVENANCE VERIFIED

Verity Record ID VTY-2026-605339A2	Execution ID a11d1302-a0eb-4791-a9c7-c645e94c50ca
Actor Communications Officer	Skill Social Draft
Risk medium	Status completed
Policy version —	Execution graph hash 1f927b14d3...bac9 Reveal Copy
Ledger entry hash 6fb1215034...a001 Reveal Copy	

Working VerityOS V0.1 product capture. Synthetic Government Communications Demo.

01 / THE INSTITUTIONAL CHALLENGE

AI capability needs institutional authority.

An institution must be able to explain which sources informed an AI output, who was allowed to request it, who approved its release, and what actually happened.

01 Which knowledge may it use?

Documents need accountable ownership, approved versions and an explicit boundary between searchable material and institutional evidence.

02 Who may authorize an action?

Roles, risk and approval rules must govern execution. A draft becoming a public communication is an institutional decision.

03 Where does the workload run?

Data location, model access and provider selection must follow the institution's deployment and information-handling requirements.

04 What evidence remains?

The request, source references, approval, exact artifact and connector outcome need a record that can be examined after the event.

VerityOS connects approved knowledge, policy controls, human decisions and recorded execution in one governed environment.

02 / ONE INSTITUTIONAL CONTROL PATH

Knowledge to evidence.

Four connected layers make AI work inspectable from the source material to the released result.



Institutional evidence begins with approval.

Uploaded means stored. Indexed means searchable. Approved means eligible as institutional evidence. These remain separate operator actions.

Institutional Guidance (Synthetic Demo)				
Sources in this collection. Only approved versions are trusted institutional evidence.				
Uploaded = file stored. Indexed = searchable. Approved = trusted institutional evidence. These stages stay separate.				
Classification internal				
Title	Versions	Approved	Indexed chunks	Created
public warning channels	1	● APPROVED	1	15 Sept 2026, 16:41 UTC
public advisory approval	7	● APPROVED	7	15 Sept 2026, 16:41 UTC
national emergency communications	12	● APPROVED	12	15 Sept 2026, 16:41 UTC
hurricane shelter operations	8	● APPROVED	8	15 Sept 2026, 16:41 UTC
government social media standard	9	● APPROVED	9	15 Sept 2026, 16:41 UTC
data classification	5	● APPROVED	5	15 Sept 2026, 16:41 UTC

Authentic capture 02, cropped for readability. Approved Institutional Guidance in the synthetic demo; not official government policy.

03 / HOW GOVERNED EXECUTION WORKS

Controls travel with the work.

Nova operates through VerityOS Core. Command defines what may happen; evidence is captured along the execution path.

01

Request & identity

Identify the organization and the actor making the request.

02

Authorization & risk

Apply permissions and classify the workflow's risk.

03

Knowledge & model routing

Retrieve eligible sources and select a policy-permitted endpoint.

04

Execution & validation

Run the governed skill and check the resulting artifact.

05

Human approval, where required

Bind the authorized decision to the exact artifact hash.

06

Action / release & audit seal

Authorize the connector, record the outcome and seal the evidence.

Audit-before-release: capture evidence as work happens. A blocked request or an ambiguous connector outcome also needs an accountable result.

04 / WORKING PRODUCT EVIDENCE

Ground the answer. Respect the boundary.

Nova research keeps approved sources and the Verity Record alongside the result. STRICT mode can stop work when the required evidence is missing.

A / GROUNDED RESEARCH

Research

Drafting

Social Draft

Question

What guidance should a communications officer follow before publishing a public emergency advisory?

Knowledge mode

grounded — cite approved sources

Knowledge collections

☒ Institutional Guidance (Synthetic Demo)

Run research

Governance

Status

Completed

Verity Record

[VTY-2026-37D642DF](#)

Citations

- government social media standard
- hurricane shelter operations
- national emergency communications · 3 chunks
- public advisory approval · 3 chunks

Capture 03: emergency-advisory question, grounded mode, approved collection and grouped citations. The demo uses mock model output, not a production model response.

B / STRICT REFUSAL

Insufficient approved evidence

● BLOCKED

No artifact.

Capture 04: insufficient approved evidence leads to BLOCKED and No artifact. The refusal is a visible policy outcome, with a Verity Record retained.

05 / HUMAN AUTHORITY

Approve the exact artifact.

Approval binds to the content's hash: its digital fingerprint. If the content changes, it is a new artifact and requires a new approval.

Awaiting approval

Social Draft

Requested by Communications Officer (communications@verity-demo.local)

mock:mock-local:SYSTEM: You are VerityOS. Follow observable skill instructions only. Do not emit

046210f586...868c [Reveal](#) [Copy](#)

You cannot approve this request. A different authorized user must approve. Self-approval is denied by Core.

Capture 05, detail: the Communications Officer sees the artifact hash and cannot approve their own request. Core enforces the restriction.

DIRECTOR / ONE APPROVAL ROW, TWO ENLARGED DETAILS

Skill	Requester	Artifact	
Social Draft	Communications Officer (communications@verity-demo.local)	046210f586...868c	Reveal Copy
	6109cd09-c...c06f	Reveal Copy	

Risk	Created	Status	Record	
medium	15 Sept 2026, 16:42 UTC	● PENDING	<u>VTY-2026-605339A2</u>	Approve Reject

Capture 06: requester and artifact above; risk, status and decision controls below. The Director can Approve or Reject. Captures 05 and 06 show the same abbreviated hash but different execution records. Release must match the approved artifact.

06 / EVIDENCE THAT CAN BE EXAMINED

A record of the path.

A Verity Record connects the actor, skill, risk, status, knowledge references, model metadata, approvals and connector evidence.

Verity Record

Verify Record

Export organization evidence

Integrity verification confirms that recorded evidence has not changed. Provenance shows the recorded path that produced the result. Neither proves factual truth. Do not read these labels as Fact Verified or Truth Verified.

● INTEGRITY VERIFIED

● PROVENANCE VERIFIED

Verity Record ID VTY-2026-605339A2	Execution ID a11d1302-a0eb-4791-a9c7-c645e94c50ca
Actor Communications Officer	Skill Social Draft
Risk medium	Status completed
Policy version —	Execution graph hash 1f927b14d3...bac9 Reveal Copy
Ledger entry hash 6fb1215034...a801 Reveal Copy	

Capture 01: verified record from the synthetic demo. The labels describe evidence checks.

INTEGRITY VERIFIED

Recorded consistency

The evidence is internally consistent under the VerityOS evidence chain and unchanged relative to the verified record.

PROVENANCE VERIFIED

Recorded origin and path

The recorded execution path corresponds to the evidence associated with the Verity Record.

Integrity and provenance verification do not prove factual truth.

They also do not establish legal sufficiency or third-party certification. V0.1 chain heads are unsigned and unanchored: an older internally consistent restore may still verify. Verification does not independently prove freshness or completeness against rollback or truncation.

07 / DEPLOYMENT AND SOVEREIGNTY

Define the boundary. Choose the environment.

VerityOS is software. Deployment can be planned for customer-controlled infrastructure, private servers or approved hosted infrastructure. Hardware procurement is a separate choice.

Customer-controlled

Operate within infrastructure controlled by the institution, with agreed responsibilities for access, backups and operations.

Approved private hosting

Use a defined hosting environment with explicit data location, access, support and model-routing arrangements.

Local or private models

The sovereign profile supports local/private routing and embeddings. Core operation does not require a cloud model provider.

Sovereignty is an operating arrangement.

Agree data location, model access, administrator authority, retention and recovery responsibilities before deployment.

V0.1 planning boundary. Production hardening may be required. Identity provisioning is operator-assisted; production SAML/OIDC is not included in V0.1. Rate limiting is process-local, and Nova is configured for one organization per process. Infrastructure determines encryption at rest. Hummingbird packaging is not validated for V0.1.

08 / GOVERNMENT COMMUNICATIONS

From guidance to an authorized release.

A focused first workflow: help a communications team prepare a public advisory using approved institutional guidance and a named approval authority.

01 Approve guidance

An owner approves institutional sources.

02 Research and draft

An Officer prepares a draft with references.

03 Authorize release

A Director approves the exact artifact.

04 Inspect the outcome

The record retains approval and action evidence.

Approval evidence

```
{
  "decided_by": "a00735ea-a504-47f5-bfeb-21b2df438724",
  "approval_id": "abb670db-e858-4706-80ec-445e2d6836df",
  "artifact_hash": "046210f58627f128225962b07f76fd6d660ed393501b3d52812e092!"
}
```

Connector / action evidence

```
{
  "action": "publish_post",
  "policy_id": "76b736ec-6f1d-4d41-86d5-4df30fa98d1a",
  "error_code": null,
  "http_class": "2xx",
  "connector_id": "1f26d734-85ae-46af-9730-641505080507",
  "artifact_hash": "046210f58627f128225962b07f76fd6d660ed393501b3d52812e092!",
  "connector_type": "meta.facebook",
  "external_action_id": "111_222",
  "policy_reason_code": "CONNECTOR_ALLOWED"
}
```

Capture 07: two enlarged details from the same completed record. Long hash fields are already clipped in the original interface. Synthetic data, mock model output and a local mock Meta service are used; this is not production Facebook publishing.

09 / PILOT PROGRAM

A defined scope. A measurable decision.

CONTROLLED INSTITUTIONAL PILOT

US\$75,000-US\$150,000

90-120 days / Typical engagement range

Start with one defined team and a bounded workflow. Agree the approved Knowledge set, roles, required approvals, deployment environment and acceptance criteria before work begins.

01 / Define

Scope, source owners, policy and baseline measures.

02 / Configure

Deployment, approved Knowledge, roles and workflow setup.

03 / Operate

Training, supervised use, refusal and approval tests.

04 / Evaluate

Evidence review, measured results and production decision.

Proposed acceptance measures

Source traceability; refusal on insufficient evidence; prevention of self-approval; exact-artifact approval and release; retrievable Verity Records; staff usability and workflow time against the agreed baseline.

Final scope and price are set by proposal. Deployment, onboarding, training and pilot support are scoped explicitly; compute, infrastructure and additional integrations must be identified in the statement of work.

10 / BEYOND THE PILOT

License the platform. Define what is yours.

Production engagements are scoped to the institution. The commercial model separates platform operation from implementation, infrastructure and specialized work.

Implementation / deployment	Environment setup, policies, Knowledge, onboarding and training.
Annual platform license	The right to operate VerityOS within the agreed deployment scope.
Support & maintenance	Agreed service levels, updates, security fixes and operational support.
Compute / model costs	Customer-provided resources, pass-through usage or an agreed allowance.
Professional services	Additional workflows, integrations, migration and custom Nova skills.

Ownership & intellectual property

Proposed contracting framework; definitive agreements govern.

INSTITUTION

Data and institutional work

The institution retains its data and source materials. Contract terms should assign rights in its outputs and records, and define export, retention and deletion.

VERITYOS

Platform and reusable IP

VerityOS retains the core software and reusable platform IP, licensed to the institution. Third-party rights remain with their owners.

Bespoke integration or workflow IP, license rights and handover obligations are agreed in the statement of work. Deployment on institutional infrastructure does not itself transfer platform source-code ownership.

Choose one workflow. Make the controls visible.

Begin with a working session for the institutional sponsor, operational owner and IT team. Define what the pilot must demonstrate and what a production decision will require.

- 01 A named workflow and accountable sponsor
 - 02 Approved sources and their institutional owners
 - 03 The people who request, review and authorize
 - 04 Deployment requirements and success measures
-

Request a pilot discussion

verityos.net/#pilot

info@verityos.net

Technical overview

V0.1 release candidate for controlled evaluation.
Product screenshots: supplied evidence pack, main 30ed98e.