DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

DAGS v1.0 Normative Standard

D3 — Security and Controls

Domain Overview

1. Purpose

This domain defines the mandatory security and control requirements that shall exist to protect the integrity, availability, and governed operation of a deployed AI system.

Its purpose is to ensure that, once an AI system is operational:

- Access to system components and control surfaces is restricted and governed
- Security controls protect against unauthorized modification or misuse
- Operational safeguards support accountable, traceable, and reconstructable system behavior
- Governance controls are enforceable through technical and procedural means
- Governance-relevant outputs and configuration states are recorded and bound to attributable authorization

This domain is normative.

---

2. Security Objective

The objective of the Security and Controls domain is to ensure that deployment-layer governance is enforceable and evidentiary.

Version: v1.0
Status: Published

Security under DAGS is not limited to protection against external threats. It includes controls that:

- Prevent unauthorized access to models, configurations, or control interfaces
- Protect the integrity of deployed behavior
- Require explicit authorization for changes meeting the definition of materially affecting behavior
- Ensure authorization decisions are recorded and attributable
- Enable version-aware traceability of outputs to exact configuration states

Security is a prerequisite for effective governance. Without enforceable controls and durable trace artifacts, governance requirements cannot be meaningfully applied.

---

3. Scope of Controls

This domain applies to all controls that materially affect the security, integrity, and governability of a deployed AI system, including:

- Access controls for system components and interfaces
- Controls governing configuration and behavior changes
- Protections against unauthorized modification or interference
- Safeguards supporting detection of security-relevant events
- Mechanisms for logging governance-relevant outputs
- Binding of configuration states to attributable authorization records

Controls may be technical, procedural, or organizational, provided they are demonstrably capable of enforcing governance requirements and producing durable, attributable evidence.

Controls that materially affect the security, integrity, or governability of the system shall be subject to documented materiality determination and governance approval requirements defined in D1 and D2.

Standards governing changes meeting the definition of materially affecting behavior apply to model versions, configuration parameters, prompt logic, integration pathways, and other mechanisms capable of altering deployed behavior.

---

4. Relationship to Other Domains

Security and Controls supports and enables:

- Governance and accountability (D1) by enforcing authority and authorization boundaries
- Model and vendor visibility (D2) by protecting version identification and dependency surfaces
- Ethics and responsible use (D4) by enabling enforceable constraint mechanisms
- Operational integration (D5) by generating the trace artifacts required for reconstruction and incident response

Without enforceable change governance, version determinism, and configuration-state binding, accountability, reconstruction capability, and ethical constraint enforcement cannot function reliably.

This domain establishes the evidentiary and enforcement substrate required for cross-domain governance integrity.

---

5. Boundary Conditions

This domain governs deployment-layer security, control, and evidentiary mechanisms, not:

- Secure software development practices
- Model training security or data protection during development
- Performance optimization or resilience engineering beyond governance needs

- Evaluation of model quality or fairness beyond enforcement of declared constraints

Such concerns are out of scope unless they directly affect deployment-layer governance, change authorization, traceability, or reconstruction capability.

---

6. Interpretive Notes

This overview provides context for the controls defined in D3_Requirements.

It does not introduce requirements, assessment logic, or examples.

Interpretation shall be governed by the normative requirements that follow.

---

7. Status

This Domain Overview is normative.

It is binding for DAGS v1.0 and all derivative artifacts unless explicitly superseded.

---

8. License & Authority

The Deployment AI Governance Standard (DAGS) is a publicly available governance standard made available for reference and implementation.

All intellectual property rights in DAGS, including the standard text, structure, methodology, and interpretive guidance, are retained by the DAGS Governing Body.

DAGS

DEPLOYMENT AI
GOVERNANCE STANDARD

Public availability of this document does not grant any license or right to use DAGS for commercial, advisory, certification, assurance, or assessment purposes. Such uses may require separate authorization or licensing from the DAGS Governing Body.

No rights are granted by implication, estoppel, or public distribution.

Editorial, interpretive, versioning, and equivalency authority is retained exclusively by the DAGS Governing Body. No third party may issue authoritative interpretations, certifications, or compliance determinations without explicit written authorization.

Deployment AI Governance Standard (DAGS) v1.0
Status: Published