DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

DAGS v1.0 Normative Standard

D3 — Security and Controls

Normative Requirements

1. Purpose

This document defines the mandatory security and control requirements for deployed AI systems under Domain D3 of the Deployment AI Governance Standard (DAGS) v1.0.

All requirements in this document are normative and binding.

---

2. Access Control

D3.1 Restricted Access

Access to deployed AI system components shall be restricted to authorized roles or functions.

Authorized access shall be documented and governed.

D3.2 Role-Based Control

Access permissions shall be assigned based on defined roles or responsibilities.

Shared, implicit, or undocumented access is prohibited.

Version: v1.0
Status: Published

3. Control of System Modification

D3.3 Controlled Modification

Mechanisms to modify system behavior, configuration, or operation shall be controlled and governed.

Unauthorized modification pathways shall not exist.

D3.4 Change Authorization

All changes meeting the definition of materially affecting behavior shall require explicit authorization in accordance with defined governance structures.

Vendor-driven updates or externally imposed modifications meeting the definition of materially affecting behavior shall require authorization and traceable documentation.

Authorization shall be attributable to an identifiable role or function.

4. Protection of System Integrity

D3.5 Integrity Safeguards

Safeguards shall exist to protect the integrity of deployed system components and configurations.

Safeguards shall be demonstrably capable of preventing or detecting unauthorized alteration within the declared operational context.

D3.6 Tamper Resistance

The deployed system shall not permit undetected modification of behavior, configuration, or control parameters.

---

5. Monitoring and Detection

D3.7 Security-Relevant Event Detection

Mechanisms shall exist to detect security-relevant events affecting system governance or integrity.

Detection shall support timely awareness of unauthorized access or modification.

D3.8 Traceability of Security Events

Security-relevant events shall be traceable to specific systems, components, and, where applicable, actors.

---

6. Credential and Secret Protection

D3.9 Protection of Credentials

Credentials, keys, or secrets that enable access to deployed AI systems shall be protected against unauthorized disclosure or use.

D3.10 Credential Lifecycle Governance

The lifecycle of credentials and access mechanisms shall be governed, including issuance, rotation, and revocation.

---

7. Segregation and Isolation

D3.11 Environment Segregation

Deployed AI systems shall be segregated from non-operational environments where necessary to protect governance integrity.

D3.12 Isolation of Control Interfaces

Control interfaces that meet the definition of materially affecting system behavior shall be isolated from general user access.

---

8. Governance-Relevant Change and Traceability Controls

D3.13 Materiality Determination

The organization shall evaluate changes to determine whether they meet the definition of materially affecting behavior.

Individuals responsible for materiality determinations shall demonstrate governance competence appropriate to system risk classification.

Changes that meet the definition of materially affecting behavior include, at minimum:

- Model version updates
- Threshold or parameter modification
- Prompt or logic modification
- Integration pathway change
- Data routing or preprocessing change

Materiality shall not be discretionary.

D3.14 Recorded Change Authorization

Authorization for changes meeting the definition of materially affecting behavior shall:

- Be documented
- Identify approving role
- Reference version/state change
- Be retained within governance records

Verbal or undocumented approval is prohibited.

D3.15 Governance-Relevant Output Logging

Deployed AI systems that influence consequential outcomes in a manner meeting the definition of materially affecting behavior shall generate logs sufficient to:

- Identify the output
- Identify timestamp
- Identify initiating actor (if applicable)
- Identify configuration state
- Identify active model version

Model version identifiers referenced under this control shall conform to D2.11 Version-Level Model Identification, and associated historical version records shall align with D2.12 Historical Version Retention.

Logged governance-relevant outputs and associated configuration-state records shall be retained in accordance with a formally defined retention schedule aligned to applicable statutes of limitation, regulatory recordkeeping requirements, and insurance policy terms, and shall not be retained for less than five years absent documented legal justification.

Model version identifiers referenced in this control shall align with D2.11 Version-Level Model Identification.

Security-only logging is insufficient.

D3.16 Configuration-State Binding

Logged outputs shall be traceable to:

- The exact configuration state active at time of output
- The authorization record governing that state

Traceability shall be established using governance-relevant logs defined in D3.15 and version-identification records defined in D2.11 and D2.12. Configuration-state references shall not rely on informal documentation, vendor-only artifacts, or undocumented system states.

---

9. Prohibited Conditions

D3.17 Uncontrolled Access Prohibited

A deployed AI system shall not operate with uncontrolled or undocumented access paths.

D3.18 Implicit Security Prohibited

Reliance on assumed security due to obscurity, vendor assurances, or informal practice shall not be considered acceptable.

---

10. Applicability

All requirements in this document apply to all deployed AI systems within DAGS scope unless explicitly stated otherwise.

---

11. Status

This Requirements document is **normative**.

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

---

12. 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