DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

DAGS v1.0 Normative Standard

DAGS Control Index

1. Purpose

This document defines the authoritative registry of control identifiers for the Deployment AI Governance Standard (DAGS) v1.0.

Its purpose is to:

- Establish a stable, canonical list of all normative controls
- Fix control identifiers and domain placement
- Prevent renumbering, reuse, or semantic drift
- Serve as the authoritative reference for all DAGS requirements

This document is normative.

---

2. Authority of the Registry

The Control Index is the authoritative source of truth for:

- Control identifiers
- Control-domain assignment
- Control existence within DAGS v1.0

If a control identifier does not appear in this index, it is not a DAGS control.

Narrative text does not supersede this registry.

---

3. Control Identifier Structure

Each control identifier follows this structure:

`D<Domain>.<Control_Number>`

Where:

- `D<Domain>` corresponds to a DAGS control domain
- `<Control_Number>` is a sequential numeric identifier within that domain

Control identifiers are stable and persistent across versions unless explicitly deprecated.

---

4. Control Domains

DAGS v1.0 defines the following control domains:

- **D1** — Governance and Accountability
- **D2** — Model and Vendor Visibility
- **D3** — Security and Controls
- **D4** — Ethics and Responsible Use
- **D5** — Operational Integration

Each control belongs to exactly one domain.

Version: v1.0
Status: Published

5. Control Index

D1 — Governance and Accountability

- D1.1 System Ownership
- D1.2 Authority to Govern
- D1.3 Accountability for Outcomes
- D1.4 Persistence of Accountability
- D1.5 Documented Governance Structure
- D1.6 Separation of Duties
- D1.7 Oversight Mechanism
- D1.8 Escalation Path
- D1.9 Retained Accountability
- D1.10 Contractual Alignment
- D1.11 Unowned Systems Prohibited
- D1.12 Implicit Governance Prohibited
- D1.13 Formal Deployment Authorization
- D1.14 Deployment Scope Declaration

D2 — Model and Vendor Visibility

- D2.1 Model Inventory
- D2.2 Model Role Clarity
- D2.3 Vendor Disclosure
- D2.4 Vendor Role Documentation
- D2.5 Behavioral Dependencies
- D2.6 Opaque Dependency Prohibition
- D2.7 Vendor Change Influence
- D2.8 Retained Authority Over Change
- D2.9 Visibility Documentation Maintenance
- D2.10 Traceability of Visibility Information

Version: v1.0
Status: Published

- D2.11 Version-Level Model Identification
- D2.12 Historical Version Retention
- D2.13 Unknown Behavioral Sources Prohibited
- D2.14 Assumed Visibility Prohibited

D3 — Security and Controls

- D3.1 Restricted Access
- D3.2 Role-Based Control
- D3.3 Controlled Modification
- D3.4 Change Authorization
- D3.5 Integrity Safeguards
- D3.6 Tamper Resistance
- D3.7 Security-Relevant Event Detection
- D3.8 Traceability of Security Events
- D3.9 Protection of Credentials
- D3.10 Credential Lifecycle Governance
- D3.11 Environment Segregation
- D3.12 Isolation of Control Interfaces
- D3.13 Materiality Determination
- D3.14 Recorded Change Authorization
- D3.15 Governance-Relevant Output Logging
- D3.16 Configuration-State Binding
- D3.17 Uncontrolled Access Prohibited
- D3.18 Implicit Security Prohibited

D4 — Ethics and Responsible Use

- D4.1 Defined Use Constraints

Version: v1.0
Status: Published

- D4.2 Documented Ethical Boundaries
- D4.2a Operationalization of Ethical Commitments
- D4.3 Assigned Ethical Accountability
- D4.4 Persistence of Ethical Accountability
- D4.5 Operational Enforcement Mechanisms
- D4.6 Human Override Capability
- D4.7 Misuse Detection and Response
- D4.8 Oversight of Ethical Compliance
- D4.9 Review and Update of Constraints
- D4.10 Constraint Transparency
- D4.11 Unconstrained Deployment Prohibited
- D4.12 Aspirational Ethics Prohibited

D5 — Operational Integration

- D5.1 Operational Embedding
- D5.2 Defined Operational Roles
- D5.3 Incident Integration
- D5.4 Accountability in Response
- D5.5 Provider Notification Obligation
- D5.6 Operational Change Management
- D5.7 Lifecycle Continuity
- D5.8 Ongoing Operational Oversight
- D5.9 Operational Reporting Paths
- D5.10 Decision Reconstruction Capability
- D5.11 Operational Readiness Requirement
- D5.12 Isolated Operation Prohibited
- D5.13 Governance by Exception Prohibited

Version: v1.0
Status: Published

6. Stability Rules

- Control identifiers shall not be reused
- Controls may be deprecated but not silently removed
- New controls shall be added only through versioned change
- Control meaning is defined by the normative requirements text

7. Relationship to Other Artifacts

- Normative requirements reference this index
- Assessment instruments map to these identifiers
- Reporting artifacts record findings against these identifiers

No artifact may introduce new identifiers.

8. Status

This Control Index is **normative**.

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

9. License & Authority

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

Version: v1.0
Status: Published

DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

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

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
Copyright © DAGS Governing Body
All Rights Reserved