DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

DAGS v1.0 Normative Standard

D4 — Ethics and Responsible Use

Normative Requirements

1. Purpose

This document defines the mandatory ethics and responsible-use requirements for deployed AI systems under Domain D4 of the Deployment AI Governance Standard (DAGS) v1.0.

This domain ensures that AI systems are operated in a manner consistent with defined operational constraints derived from ethical and responsible-use commitments.

All requirements in this document are normative and binding.

---

2. Definition and Operationalization of Ethical and Responsible-Use Constraints

D4.1 Defined Operational Use Constraints

Each deployed AI system shall have explicitly defined operational constraints derived from ethical and responsible-use commitments that govern permissible use.

Constraints shall:

- Be specific to the deployed system and its declared operational context
- Be traceable to the declared system scope

- Be expressed in measurable or enforceable terms appropriate to the system's risk classification

Implicit or assumed ethical boundaries are prohibited.

D4.2 Documented Ethical Boundaries

Ethical and responsible-use boundaries shall be documented in a manner that is accessible to those governing and operating the system.

Documentation shall enable:

- Enforcement
- Oversight
- Reconstruction of decisions
- Independent review

D4.2a Operationalization of Ethical Commitments

Ethical and responsible-use commitments shall be translated into measurable governance principles, including where applicable:

- Transparency of system purpose, intended use, and limitations
- Explainability or interpretability appropriate to system risk
- Fairness and non-discrimination safeguards
- Accuracy and performance monitoring obligations
- Human oversight and intervention capability

These principles shall be instantiated as enforceable deployment-layer controls.

Abstract ethical declarations without measurable instantiation are prohibited.

3. Governance of Ethical Responsibility

D4.3 Assigned Ethical Accountability

Accountability for defining, maintaining, and enforcing ethical and responsible-use constraints shall be explicitly assigned.

The accountable role or function shall:

- Be identifiable and documented
- Demonstrate documented governance competence appropriate to the system's risk classification

Competence may include training, certification, demonstrated governance experience, or other verifiable qualifications.

D4.4 Persistence of Ethical Accountability

Ethical accountability shall persist across:

- System updates
- Configuration changes
- Vendor transitions
- Operational handoffs

Changes in personnel or vendors shall not result in unassigned ethical responsibility.

---

4. Enforcement of Responsible Use

D4.5 Operational Enforcement Mechanisms

Mechanisms shall exist to enforce defined ethical and responsible-use constraints at the deployment layer.

Enforcement mechanisms shall be demonstrably capable of preventing or materially limiting prohibited uses within the declared operational context.

Evidence shall document how enforcement capability was evaluated relative to foreseeable misuse scenarios.

Symbolic or non-functional enforcement mechanisms are prohibited.

D4.6 Human Override Capability

For systems influencing consequential decisions in a manner meeting the definition of materially affecting behavior:

- A documented human override or intervention mechanism shall exist
- Override capability shall be operationally accessible
- Override authority shall be assigned and governed

Override mechanisms shall be capable of interrupting, constraining, or halting system behavior where necessary to prevent or mitigate harm.

D4.7 Misuse Detection and Response

Mechanisms shall exist to detect foreseeable misuse of the deployed AI system and to enable timely response or mitigation.

Detection mechanisms shall support governance action, including:

- Investigation
- Intervention
- Constraint modification

Misuse detection shall not be purely reactive where foreseeable misuse can be reasonably anticipated.

---

5. Oversight and Review

D4.8 Oversight of Ethical Compliance

Oversight mechanisms shall exist to monitor adherence to ethical and responsible-use constraints.

Oversight shall:

- Be assigned and documented
- Include review authority independent from routine operational monitoring
- Be capable of initiating corrective action

Oversight shall include periodic reassessment of whether defined constraints remain sufficient given evolving system behavior and operational context.

D4.9 Review and Update of Constraints

Ethical and responsible-use constraints shall be reviewed when changes meeting the definition of materially affecting behavior occur to system behavior, operational context, integrations, or risk profile.

Vendor model updates, externally imposed behavioral modifications, or integration changes meeting the definition of materially affecting behavior shall trigger review.

Reviews shall not be discretionary when changes are material.

Evidence of review and resulting determinations shall be retained.

---

6. Transparency of Constraints

D4.10 Constraint Transparency

Ethical and responsible-use constraints shall be transparent to relevant internal stakeholders responsible for system governance and operation.

Transparency shall:

- Support enforcement
- Enable accountability
- Prevent hidden or undocumented constraint regimes

Transparency does not require public disclosure unless otherwise mandated.

---

7. Prohibited Conditions

D4.11 Unconstrained Deployment Prohibited

A deployed AI system shall not operate without defined and enforceable operational constraints derived from ethical and responsible-use commitments.

D4.12 Aspirational Ethics Prohibited

Statements of values, principles, or intent shall not substitute for defined and enforceable responsible-use controls.

Ethical commitments that are not operationalized into measurable deployment-layer controls shall not be represented as governed.

---

8. Applicability

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

---

9. Status

This Requirements document is normative.

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

---

10. 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.

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