DAGS

DEPLOYMENT AI GOVERNANCE STANDARD

DAGS v1.0 Normative Standard

D3 — Security and Controls

Evidence Principles

1. Purpose

This document defines the **evidence principles** applicable to the Security and Controls domain (D3) of the Deployment AI Governance Standard (DAGS) v1.0.

Its purpose is to:

- Specify the nature and category of evidence required to demonstrate satisfaction of D3 requirements
- Ensure security evidence supports enforceable governance, not aspirational posture
- Prevent substitution of assumed security or vendor claims for demonstrable controls

This document is normative.

---

2. General Evidence Standard

Evidence for D3 requirements shall demonstrate that security and control mechanisms exist and are enforceable at the deployment layer.

Evidence shall be:

- Documented and durable

- Attributable to the declared system scope
- Sufficient to demonstrate control over access, modification, and integrity
- Current with respect to the deployed system

Claims of security without supporting artifacts are insufficient.

---

3. Access Control Evidence

Evidence demonstrating access control shall establish:

- That access to system components is restricted
- That access permissions are role-based and documented
- That unauthorized access paths are not permitted

Acceptable evidence categories include:

- Access control policies or role definitions
- System access configuration records
- Documentation linking roles to access permissions

Informal or assumed access restrictions are not acceptable.

---

4. Change Control Evidence

Evidence of controlled system modification shall demonstrate:

- Existence of mechanisms governing changes to system behavior or configuration
- Requirement for explicit authorization prior to material changes
- Attribution of authorization to identifiable roles or functions

Acceptable evidence categories include:

- Change authority documentation
- Change approval records or logs
- Governance procedures governing system modification

Evidence of monitoring alone does not satisfy change control requirements.

---

5. Integrity Protection Evidence

Evidence supporting system integrity shall demonstrate:

- Safeguards protecting deployed components and configurations
- Ability to detect or prevent unauthorized modification
- Protection of control surfaces affecting system behavior

Acceptable evidence categories include:

- Integrity protection mechanisms documentation
- Configuration management records
- System control protection descriptions

Integrity shall not be inferred from absence of known incidents.

---

6. Monitoring and Detection Evidence

Evidence for monitoring and detection shall demonstrate:

- Existence of mechanisms to detect security-relevant events

- Ability to identify events affecting governance or integrity
- Traceability of events to systems and components

Acceptable evidence categories include:

- Monitoring or detection system descriptions
- Event logging configurations
- Records demonstrating detection capability

Logs without defined purpose or attribution are insufficient.

---

7. Credential and Secret Management Evidence

Evidence supporting credential protection shall demonstrate:

- Protection of credentials enabling system access
- Governance of credential lifecycle activities
- Ability to revoke or rotate credentials when necessary

Acceptable evidence categories include:

- Credential management policies
- Access key governance documentation
- Records of credential lifecycle controls

Embedded or unmanaged secrets are not acceptable.

---

8. Segregation and Isolation Evidence

Evidence of segregation and isolation shall demonstrate:

- Separation of operational systems from non-operational environments where required
- Isolation of control interfaces from general access

Acceptable evidence categories include:

- Environment architecture documentation
- Access boundary definitions
- Control interface restriction records

Segregation shall not be implied by convention.

---

9. Prohibited Evidence Substitutions

The following shall not be accepted as evidence for D3 requirements:

- Vendor security whitepapers without system linkage
- Statements of compliance with security standards
- Assumptions of security based on platform choice
- General organizational security policies not tied to the system

Such materials do not demonstrate deployment-layer security controls.

---

10. Status

This Evidence Principles document is **normative**.

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

---

11. 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