

01 · TEMPLATE · VERSION 1.0 · OCTOBER 2026

Agent Access Standard

How AI agents may sign in to, read from and act in organizational systems.

HOW TO USE THIS TEMPLATE

Replace every [bracketed] item with your own. Delete any pattern your organization won't allow. Keep the crosswalk in section 13, because it shows where each requirement comes from. Have your security lead and system owners review sections 6 and 7 before you adopt it.

01

Purpose

This standard sets how AI agents get access to [Organization]'s systems and data, who approves that access, and what gets recorded. It exists so that every agent action can be traced to an agent, to the person it acted for, and to the decision that allowed it.

02

Scope

It applies to any AI agent that signs in to, reads from or takes action in a system that [Organization] owns or operates, or that handles [Organization] data, on behalf of a person or of the organization. That includes assistants, browser agents and coding agents, whether built in-house, bought, or brought by staff.

AI tools that only see what a person pastes into them are covered by [Acceptable Use Policy] instead.

Definitions

TERM	MEANING
Agent	Software that uses an AI model to decide on and take actions in a system with some independence.
Principal	The person or organizational role on whose behalf an agent acts.
Grant	A recorded permission for one agent to reach one system, for one principal, under one pattern.
Brokered sign-in	A credential manager or broker fills the principal's credential into the sign-in flow after the principal approves. The agent never receives the credential.
Delegated identity	The agent signs in as itself and carries a token that names both the agent and the principal, with scopes no wider than the task needs.
Model endpoint	The service where the agent's model runs. Everything the agent reads, including page content after sign-in, is sent there.
Authorized boundary	The systems and services approved to process a given class of data under [Organization]'s authorization documents, such as [system security plan].
Controlled data	Data with handling rules set by law, regulation, contract or policy, such as Controlled Unclassified Information.
High-impact action	An action that can't be undone, spends money, sends information outside [Organization], changes access, or deletes records.
Step-up approval	A fresh, specific human approval for one high-impact action, given just before it runs.

Roles

R does the work, A owns the decision, C is consulted, I is informed. Rename the roles to match your organization.

ACTIVITY	PRINCIPAL	SYSTEM OWNER	SECURITY LEAD	AI GOVERNANCE LEAD	ACCOUNTABLE EXECUTIVE
Register an agent	R	I	C	A	I
Approve a Pattern A grant	R	A	C	I	
Approve a Pattern B grant	R	A	R	C	I
Confirm the model endpoint is inside the boundary		C	A	C	I
Accept risk for high-impact use or an exception	I	R	C	C	A
Review the register		C	C	A	I
Revoke a grant	R	A	R	I	I

The accountable executive is the person who owns AI risk for [Organization], such as a Chief AI Officer. Anyone in these roles may revoke a grant at once. Restoring access takes a new grant.

Requirements

- 5.1 Agents shall not receive, store or view a person's password, one-time code or other authenticator.
800-171 r3 03.05.12 · OWASP §2.2.1, KC6.6
- 5.2 Each agent shall be registered in the Agent Access Register before it reaches any system.
CoSAI §3.2 · AI RMF GOVERN 1.6 · M-25-21 §3(a)(i)(E)
- 5.3 Each grant shall name one agent, one principal, one system and one pattern.
800-171 r3 03.05.01 · CoSAI §1.2
- 5.4 Agent access shall default to read-only. Write, send, purchase and delete permissions shall be granted separately and listed by name.
800-171 r3 03.01.05 · OWASP §4.1.1

-
- 5.5 Every grant shall have an end date. A grant without one is invalid.
CoSAI §1.2 · OWASP §3.2.8
-
- 5.6 Data shall reach a model endpoint only when that endpoint is inside the authorized boundary for that class of data.
800-171 r3 03.01.03, 03.01.20
-
- 5.7 High-impact actions shall need step-up approval, unless the grant lists the action as pre-approved and the accountable executive accepted that risk.
CoSAI §3.4 · M-25-21 §4(b)(v) · AI RMF MAP 3.5
-
- 5.8 For every Pattern B grant, logs shall let a reviewer tell the agent's actions from the principal's.
800-171 r3 03.03.02 · CoSAI §1.2 · OWASP §7.2
-
- 5.9 When a required check can't run, access shall be denied.
CoSAI §5.1
-
- 5.10 Any role in section 4 shall be able to revoke a grant in one step.
AI RMF MANAGE 2.4 · OWASP §4.1.4
-

06

Access patterns

Every grant uses exactly one of these patterns. A system can allow different patterns for different agents, and the register records which.

A Brokered sign-in

The agent signs in as the principal through a credential manager or broker. The principal approves each use on their own device and sees which credential is requested and why. The system and its logs see the principal.

USE FOR

- Accounts and systems that hold no controlled data
- Read-only work
- Systems whose owner accepts that logs will show only the principal

NEVER FOR

- Controlled data
- Any system whose audit records must identify the agent
- High-impact actions

REQUIRED CONTROLS

- Approval for each use, showing the credential and the reason
- The agent never receives the credential
- The session ends when the task ends (800-171 r3 03.01.11)
- The agent keeps no session between tasks (OWASP §5.5)

B Delegated identity

The agent has its own identity in [identity provider]. For each task it receives a short-lived token that names the agent as actor and the principal as subject, with scopes no wider than the task needs and never wider than the principal's own.

USE FOR	NEVER FOR	REQUIRED CONTROLS
<ul style="list-style-type: none">• Organizational systems• Anything that writes, sends, buys or deletes• Systems assessed for attribution	<ul style="list-style-type: none">• Controlled data whose model endpoint sits outside the authorized boundary	<ul style="list-style-type: none">• A distinct identifier for the agent (800-171 r3 03.05.05)• Tokens carry both actor and subject (CoSAI appendix on token claims; RFC 8693)• Scopes narrow at each hop and never expand (CoSAI §3.4)• Token lifetime of [minutes]• Logging as in section 9• Step-up approval for high-impact actions• Revoking the delegation cuts off everything downstream

C No agent access

The system is closed to agents.

USE FOR	REQUIRED CONTROLS
<ul style="list-style-type: none">• Controlled data, until the agent and its model endpoint are both inside the authorized boundary and documented in [system security plan]• Any system whose owner has not approved a grant	<ul style="list-style-type: none">• The system owner marks the system as closed in the register• A technical block where the system supports one, such as [conditional access rule]

Choosing a pattern

Answer these six questions in the grant record before access starts. Stop at the first answer that settles the pattern.

QUESTION	IF THE ANSWER IS	THEN
1. Where does the model run, and is it inside the authorized boundary for this data?	Outside, and the data is controlled	Pattern C. Stop.
2. Will the agent only read?	It writes, sends, buys or deletes	Pattern B.
3. Must the log identify the agent apart from the principal?	Yes	Pattern B.
4. Which scopes does it need, and which are excluded?	Any answer	Record both. Anything not listed is denied.
5. When does access end, and who revokes it?	Any answer	Record the end date and the steps. No end date, no grant.
6. Which actions need a person every time?	Any answer	List them. Keep the list to high-impact actions so each prompt still gets read (OWASP §5.6).

If questions 1 to 3 don't require Pattern B or C and the system owner agrees, Pattern A is allowed.

Grant record

The Agent Access Register holds one row per grant with these fields.

FIELD	WHAT TO RECORD
Grant ID	A unique ID, never reused.
Agent and agent owner	The agent's name and identifier, and the person responsible for it.
Model and endpoint location	The model and where it runs, including the hosting service and region.
Inside boundary	Yes or no for this data class, and who confirmed it.

Principal	The person or role the agent acts for.
System and resources	The system, and the resources within it the agent may reach.
Data class	The highest class of data the agent can reach through this grant.
Pattern	A, B or C.
Scopes allowed and excluded	Both lists, by name.
High-impact actions	Each one, and whether it needs step-up approval or was pre-approved.
Approver and date	Who approved the grant, and when.
Risk accepted by	Required for any pre-approved high-impact action or exception.
Start and end dates	Both required.
Revocation steps	What to disable, and where.
Log location	Where the records in section 9 are kept.
Next review	The date of the next review.

09

Logging

For every action under a Pattern B grant, and under Pattern A wherever the system allows it, record:

FIELD	CONTENTS
Agent	Agent identifier
Acting for	Principal identifier
Where	System, tenant, environment and resource
What	The action requested or taken
Decision	Allowed or denied, with the reason
Approval	Approver and time, when a person approved or denied it
Rule	Policy version applied

- Never log tokens, passwords or one-time codes (OWASP §3.3.3).
 - Keep logs where the agent can't change them (800-171 r3 03.03.08).
 - Record every human approval and denial with the approver's name (OWASP §3.1.5).
 - Keep logs for [retention period] and review them [frequency] (800-171 r3 03.03.05).
-

10

Revocation and decommissioning

Revoke a grant when any of these happens:

- The end date arrives.
- The principal changes role or leaves.
- The agent, its model or its model endpoint changes.
- Logs show an action outside the grant's scopes.
- The system owner, the security lead or the accountable executive asks.

To revoke: disable the agent's identity or remove its approval in the credential manager, revoke active tokens and sessions, confirm downstream delegations are cut, then record the date and reason in the register. Keep the logs for the full retention period.

11

Review

The AI governance lead reviews the register [quarterly] and reports to the accountable executive on active grants by pattern, expired grants still active, grants past their review date, and open exceptions.

Review sooner after an incident, when a vendor changes how its agents sign in, or when an agent moves to a new model endpoint.

12

Exceptions

An exception is written, lasts no longer than [90] days, names its compensating controls, and is accepted by the accountable executive. It is recorded in the register. No exception lets an agent receive a person's authenticator.

Crosswalk

Mappings are the author's reading of each source. Confirm them against your own authorization documents before relying on them.

FEDERAL REQUIREMENTS

REQ.	NIST SP 800-171 R3	CMMC LEVEL 2	CMMC LEVEL 3	OMB M-25-21
5.1	03.05.12 Authenticator Management			
5.2	03.01.01 Account Management; 03.05.05 Identifier Management	AC.L2-3.1.1	IA.L3-3.5.3e; CM.L3-3.4.3e	§3(a)(i)(E) AI use case inventory
5.3	03.05.01 User Identification and Authentication	IA.L2-3.5.1	IA.L3-3.5.1e	
5.4	03.01.02 Access Enforcement; 03.01.05 Least Privilege	AC.L2-3.1.2; AC.L2-3.1.5		
5.5	03.01.01 Account Management	AC.L2-3.1.1		
5.6	03.01.03 Information Flow Enforcement; 03.01.20 Use of External Systems	AC.L2-3.1.3; AC.L2-3.1.20	AC.L3-3.1.2e; AC.L3-3.1.3e	n.22: AI risk acceptance doesn't replace system authorization
5.7	03.05.01(b) re-authentication for privileged functions			§4(b)(v) human oversight and fail-safe
5.8	03.03.01 Event Logging; 03.03.02 Audit Record Content; 03.03.08 Protection of Audit Information	AUL2-3.3.1; AUL2-3.3.2; AUL2-3.3.8		§4(b)(iii) monitoring, traceability
5.9	03.01.02 Access Enforcement	AC.L2-3.1.2	IA.L3-3.5.3e	§4(b)(v) fail-safe
5.10	03.01.01 Account Management; 03.01.11 Session Termination	AC.L2-3.1.1; AC.L2-3.1.11		

AI GOVERNANCE FRAMEWORKS

REQ.	ISO/IEC 42001 ANNEX A	NIST AI RMF 1.0	COSAI AGENTIC IAM	OWASP AGENTIC GUIDANCE
5.1		MEASURE 2.7	§5.2 eliminate shared accounts	§2.2.1; KC6.6
5.2	A.4.4 Tooling resources	GOVERN 1.6	§3.2; §5.2	§3.1.8
5.3	A.3.2 AI roles and responsibilities; A. 10.2 Allocating responsibilities	GOVERN 3.2	§1.2 (1)	§3.1.8

REQ.	ISO/IEC 42001 ANNEX A	NIST AI RMF 1.0	COSAI AGENTIC IAM	OWASP AGENTIC GUIDANCE
5.4	A.9.2 Processes for responsible use of AI	MAP 4.2	§3.1	§4.1.1; §5.1
5.5			§1.2 (2) zero standing privilege; §3.5	§3.2.8
5.6	A.10.3 Suppliers	GOVERN 6.1	§3.1	§5.4
5.7	A.9.2 Processes for responsible use of AI	MAP 3.5	§3.4	§3.1.5; §5.6; T10
5.8	A.6.2.8 AI system recording of event logs	MEASURE 2.8	§1.2 (3), (6); log fields appendix	§7.2; T8; T9
5.9	A.6.2.6 AI system operation and monitoring	MANAGE 2.4	§5.1	
5.10	A.6.2.6 AI system operation and monitoring	MANAGE 2.4; GOVERN 1.7	§3.4; §3.5	§4.1.4

Notes. CMMC Level 2 tests the NIST SP 800–171 Rev 2 requirements, so Level 2 IDs follow Rev 2 numbering. Level 3 adds selected NIST SP 800–172 requirements on top of a Final Level 2 (C3PAO) status, so a Level 3 cell adds to the Level 2 cell beside it. OMB M–25–21 applies to federal agencies and excludes National Security Systems. ISO/IEC 42001 is cited by control title only. A blank cell means the source has no close match.

Sources

- NIST SP 800–171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, May 2024.
- CMMC Assessment Guide, Level 2, Version 2.13, September 2024.
- CMMC Assessment Guide, Level 3, Version 2.13, September 2024.
- OMB M–25–21, Accelerating Federal Use of AI through Innovation, Governance, and Public Trust, April 3, 2025.
- ISO/IEC 42001:2023, Artificial intelligence: Management system.
- NIST AI 100–1, Artificial Intelligence Risk Management Framework (AI RMF 1.0), January 2023.
- Coalition for Secure AI (OASIS), Agentic Identity and Access Management, Version 1.0, March 20, 2026.
- OWASP GenAI Security Project, Securing Agentic Applications Guide 1.0, July 28, 2025.
- OWASP GenAI Security Project, State of Agentic AI Security and Governance 1.0, July 2025.
- 1Password, "1Password for Agents," press release, October 22, 2026.

Template by Jerome Davis, ISO/IEC 42001 Lead Auditor. Free to copy and adapt. The editable version and the Agent Access Register are free at secondorderstrategy.com. It is a starting point and is not legal or compliance advice.