

Standards Body · Institutional-design proposal, public edition · Released July 17, 2026
Canonical record: <https://standardsbody.ai/library/institutional-design/partnership-principles/>
Standards Body is an independent research and institutional-design project. It is not currently a regulator, accreditation body, certification body, or governmental authority. This document is research; it is not an adopted standard.

PARTNERSHIP_PRINCIPLES.md

Standards Body Partnership Principles

Project: Standards Body

Primary domain: standardsbody.ai

Core line: Foundations for Frontier AI

Document type: Canonical partnership-governance, due-diligence, independence, public-interest, funding, data, intellectual-property, security, branding, transparency, monitoring, and exit framework

Version: 1.0

Status: Approved foundational source

Document owner: Standards Body

Present institutional stage: Independent foundational research and institutional design

Applies to: Research collaborations, standards liaisons, government relationships, evaluator and accreditation relationships, industry collaborations, model-access agreements, civil-society partnerships, academic partnerships, philanthropic funding relationships, international cooperation, regional partnerships, technical infrastructure arrangements, data-sharing agreements, joint publications, public-interest collaborations, vendors, contractors, sponsors, and future institutional alliances

Related canonical sources: PROJECT_IDENTITY.md, PROJECT_MANIFESTO.md, INSTITUTION_DESIGN.md, GOVERNANCE_FRAMEWORK.md, STANDARDS_DEVELOPMENT_PROCESS.md, EVALUATOR_ACCREDITATION_FRAMEWORK.md, TRANSPARENCY_FRAMEWORK.md, CONTRIBUTOR_FRAMEWORK.md, WEBSITE_SOURCE_OF_TRUTH.md, SOURCES.md, VERSION_HISTORY.md, TERMINOLOGY.md, TAXONOMY.md, EVIDENCE_STANDARDS.md, RESEARCH_METHODOLOGY.md, EVALUATION_PHILOSOPHY.md, FOUNDATIONS.md, FOUNDATIONS_APPENDIX.md, and the eight foundation papers

Research basis reviewed through: July 16, 2026

Review cycle: Annual complete review, quarterly material-partnership review, and event-triggered revision after a material partnership incident, authority change, funding conflict, standards-process change, security failure, human-rights concern, legal change, international-recognition change, or institutional-stage transition

Authority Note

This document governs how Standards Body should evaluate, approve, describe, operate, monitor, correct, renew, and end partnerships.

It does not establish that:

- Standards Body is authorized to represent any partner
- a partner is authorized to represent Standards Body
- a partnership creates endorsement
- a partnership creates membership
- a partnership creates certification
- a partnership creates accreditation
- a partnership creates legal recognition
- a partnership creates governmental authority
- a partnership creates an international mandate
- participation creates consensus
- funding creates ownership
- model access creates evaluation independence
- a memorandum of understanding creates binding public authority
- a logo exchange creates institutional equivalence
- a liaison relationship creates voting rights
- a research collaboration creates approval of the partner's products, policies, or conduct
- a government relationship converts Standards Body into a public authority
- a standards relationship converts Standards Body into a formally recognized standards-development organization
- a relationship with an accreditation body makes Standards Body an accreditation body
- a relationship with an evaluator makes Standards Body an evaluator
- a relationship with a developer validates the developer's safety claims

Standards Body remains an independent research and institutional-design project unless a lawful, competence-based, transparently governed, and publicly recorded transition establishes a different role.

Every partnership should preserve that boundary.

Where a partner's public description conflicts with the approved relationship, Standards Body should require correction.

If correction is not made promptly, Standards Body should suspend use of its name, mark, or affiliation and consider termination.

Canonical Partnership Position

A partnership should exist only when it advances a defined public-interest purpose that neither party could achieve as well alone, while preserving independent

judgment, bounded authority, transparent roles, lawful information handling, and a credible right to disagree, correct, suspend, and exit.

The defining partnership rule is:

Collaborate on the work without surrendering the judgment.

Document Purpose

This framework establishes the complete partnership system for Standards Body.

It defines:

- What constitutes a partnership
- what does not constitute endorsement
- partner categories
- relationship types
- partnership tiers
- authority and approval
- eligibility
- due diligence
- mission alignment
- public-interest review
- human-rights due diligence
- independence
- conflict-of-interest control
- funding
- resource contributions
- government relationships
- standards relationships
- evaluator, certification, and accreditation relationships
- developer and model-provider relationships
- academic and research relationships
- civil-society and affected-community relationships
- international and regional cooperation
- philanthropic relationships
- open-source and technical-community relationships
- vendor and contractor relationships
- data sharing
- model and system access
- intellectual property
- publication rights
- confidentiality
- security
- privacy
- branding

- logos and marks
- public statements
- joint governance
- decision rights
- agreements
- antitrust and competition
- anti-corruption
- sanctions and export controls
- political independence
- accessibility
- language and regional equity
- monitoring
- complaints
- incidents
- corrections
- renewal
- suspension
- termination
- post-exit obligations
- records
- public registries
- metrics
- audits
- failure modes
- implementation
- operational templates

The framework is designed for an institution whose value depends on credible independence.

Standards Body may need partners to obtain:

- Technical expertise
- model access
- protected evidence
- evaluator capacity
- standards coordination
- legal knowledge
- international participation
- regional understanding
- public-interest representation
- research funding
- computing infrastructure
- implementation experience
- archival continuity
- translation
- accessibility

- dissemination

Those resources can strengthen the work.

They can also distort it.

A model provider may offer access while controlling publication.

A funder may support independence while shaping priorities.

A government may provide recognition while creating political pressure.

A standards organization may offer legitimacy while limiting participation.

An evaluator may provide expertise while benefiting from the requirements being drafted.

A civil-society organization may provide affected-party knowledge while carrying advocacy commitments.

An academic institution may provide expertise while lacking operational continuity.

An international partner may expand reach while creating false claims of global representation.

Partnership governance should not assume that one category is inherently independent or compromised.

It should examine the actual relationship.

Executive Summary

Standards Body should build a network, not a dependency chain.

Partnerships are necessary because frontier AI standards, evaluation, assurance, and governance cannot be developed credibly by one institution acting alone.

The required capabilities are distributed across:

- Research institutions
- governments
- standards organizations
- evaluators
- accreditation bodies
- certification bodies
- developers
- cloud and infrastructure providers
- civil society
- affected communities
- labor
- professional associations
- philanthropy

- international institutions
- regional organizations
- open-source communities

A partnership can improve:

- Evidence
- competence
- implementation
- interoperability
- legitimacy
- access
- capacity
- geographic coverage
- language coverage
- accountability

A partnership can also create:

- Capture
- authority inflation
- logo laundering
- funder dependence
- access dependence
- publication control
- data misuse
- intellectual-property lock-in
- exclusion
- anticompetitive coordination
- political influence
- security exposure
- reputational contagion
- false endorsement

The purpose of this framework is to permit useful collaboration while preventing those harms.

Partnership Is Not One Relationship Type

The word **partner** is too broad to govern responsibly.

Standards Body should identify the exact relationship.

Examples:

- Research collaborator
- standards liaison
- model-access provider
- data provider

- evaluator collaborator
- accreditation liaison
- public-interest advisor
- funder
- sponsor
- infrastructure provider
- contractor
- memorandum party
- implementation pilot host
- government advisor
- regional convening partner
- translation partner
- publication collaborator
- joint-project participant

Each relationship creates different rights, risks, and public meanings.

Material Partnership Test

A relationship is material when it could reasonably affect:

- Standards Body's mission
- institutional authority
- public credibility
- research priorities
- standards outcomes
- evaluation independence
- funding concentration
- access to frontier systems
- confidential information
- security
- intellectual property
- international representation
- public claims
- affected communities
- the ability to exit

Material partnerships require enhanced review and public disclosure.

Core Partnership Requirements

Every material partnership should have:

- A defined public-interest purpose
- a precise relationship type
- approved authority

- due diligence
- conflict review
- funding disclosure
- decision-rights boundaries
- publication rights
- data and intellectual-property terms
- security and privacy controls
- brand and public-claims rules
- monitoring
- complaint and incident routes
- termination rights
- post-exit obligations
- a public summary

No Implied Endorsement

A partnership should not imply that:

- Standards Body endorses every activity of the partner
- the partner endorses every Standards Body position
- the parties have merged
- the partner can speak for Standards Body
- Standards Body has approved a partner's AI system
- a government has delegated authority
- an international institution has recognized Standards Body
- an evaluator is accredited
- a developer's claims are independently verified

Developer and Model-Provider Partnerships

Relationships with frontier AI developers require enhanced review because access can become leverage.

The agreement should state:

- Which system is accessible
- which version
- which access mode
- which restrictions
- who controls task design
- whether publication is independent
- whether factual review is allowed
- whether approval rights exist
- what happens after adverse findings
- whether access can be withdrawn
- whether unrelated access can be threatened

- whether funding is provided
- whether personnel are shared
- whether results may be used in marketing

The developer may review reports for:

- Confidentiality
- security
- factual system identity
- technical errors

The developer should not control:

- Conclusions
- scoring
- evidence interpretation
- publication solely because findings are unfavorable
- correction of independently supported criticism

Government Partnerships

A government relationship should identify whether it is:

- Informal consultation
- research
- advisory
- contractual
- procurement
- grant funded
- recognized
- delegated
- regulatory
- enforcement related

Standards Body should not describe a government relationship in terms suggesting legal authority unless the authority actually exists.

Standards Relationships

Standards Body should cooperate with standards organizations to reduce duplication and improve interoperability.

Liaison status should be described according to the actual procedural rights.

Participation in an ISO, IEC, national, regional, or other standards process does not automatically establish:

- Voting rights

- consensus
- adoption
- recognition
- ownership
- international-standard status

The ISO/IEC Directives distinguish members, delegates, experts, and liaison organizations, and provide specific conditions for participation.[^iso-directives]

Human Rights and Affected Parties

The United Nations Guiding Principles on Business and Human Rights emphasize human-rights due diligence, meaningful engagement, and remedy.[^ungp]

Partnership due diligence should examine whether the relationship may:

- Cause adverse impact
- contribute to adverse impact
- become directly linked to adverse impact
- obstruct affected-party participation
- expose human-rights defenders
- create retaliation
- deny remedy

A technically useful partnership should not proceed unchanged where severe public-interest harms remain unaddressed.

International Standards Principles

The WTO Technical Barriers to Trade Committee's principles for international standards include:

- Transparency
- openness
- impartiality and consensus
- effectiveness and relevance
- coherence
- the development dimension[^wto-six]

These principles should guide Standards Body's standards partnerships.

They should not be used to claim that Standards Body is already an international standardizing body.

Funding

Funding should purchase defined work or support the mission.

It should not purchase:

- Conclusions
- standards outcomes
- favorable evaluation
- governance seats
- permanent veto
- publication approval
- privileged complaint treatment
- concealed agenda control

Exit

A partnership without a credible exit right can become an institutional dependency.

Agreements should permit suspension or termination after:

- Mission conflict
- interference
- corruption
- misconduct
- human-rights harm
- security failure
- false public claims
- concealed conflict
- unlawful activity
- retaliation
- repeated failure to correct

Exit should protect:

- Records
- evidence
- contributors
- affected parties
- published work
- correction rights
- confidential information
- continuity

Final Partnership Proposition

The strongest partnership is not the closest institutional association. It is the relationship in which each party's role is precise, each contribution is useful, each conflict is governed, each public claim is bounded, and each party remains free to report the truth and leave.

1. Foundational Partnership Principles

1.1 Mission Before Opportunity

A prestigious or well-funded opportunity should not override mission.

1.2 Public Purpose

Every material partnership should identify the public-interest outcome it is intended to advance.

1.3 Bounded Relationship

The relationship should be described by actual function, not a broad prestige label.

1.4 Independent Judgment

No partner should control Standards Body's technical, evidentiary, editorial, or governance conclusions beyond legitimate agreed procedures.

1.5 No Implied Endorsement

Collaboration on one activity does not imply approval of all activities.

1.6 Authority Precision

A partnership should not imply legal, governmental, standards, certification, accreditation, or international authority that does not exist.

1.7 Reciprocity Without Equivalence

Parties may exchange access, expertise, funding, or recognition without becoming institutionally equivalent.

1.8 Proportionate Due Diligence

Review should scale with consequence, dependence, sensitivity, duration, and public meaning.

1.9 Human-Rights Responsibility

Technical value does not excuse foreseeable severe harm.

1.10 Conflict Visibility

Material interests should be disclosed and governed.

1.11 Publication Integrity

Partners may correct factual errors and protect legitimate secrets.

They should not suppress supported conclusions.

1.12 Data and Security Discipline

Access to data or systems should be lawful, necessary, controlled, and reviewable.

1.13 Intellectual Independence

Funding and access should not create ownership of institutional positions.

1.14 Nonexclusivity by Default

Exclusive relationships require strong public-interest justification.

1.15 Correctable Public Claims

Misleading partner descriptions should be corrected promptly.

1.16 Time-Bounded Commitment

Material partnerships should have review, renewal, and exit dates.

1.17 Partnership Pluralism

Standards Body should avoid dependence on one government, developer, evaluator, funder, region, or intellectual tradition.

1.18 Affected-Party Voice

People affected by the work should have meaningful routes to inform, challenge, and seek remedy.

1.19 Lawful Cooperation

Partnerships should comply with applicable law, including competition, anti-corruption, sanctions, export control, privacy, employment, and intellectual-property obligations.

1.20 Preserved History

The partnership record should remain available after the relationship ends.

2. Scope and Non-Claims

2.1 Covered Relationships

- Formal partnerships
- memoranda of understanding
- joint projects
- research collaborations
- standards liaisons
- grants
- sponsorships
- data-sharing arrangements
- model-access agreements
- infrastructure arrangements
- evaluator collaborations
- government advisory relationships
- international cooperation
- regional hubs
- implementation pilots
- joint publications
- vendor relationships with material institutional effect

2.2 Ordinary Transactions

An ordinary purchase may not require partnership treatment.

It becomes partnership-like when it creates:

- Public association
- strategic dependence
- joint governance
- data sharing
- confidential access
- mission influence
- branding
- substantial funding
- long duration

2.3 Contributor Relationships

Individual contributor roles are governed primarily by `CONTRIBUTOR_FRAMEWORK.md`.

An institutional contribution may also be a partnership.

2.4 Membership

Membership, participation, partnership, liaison, sponsorship, and service provision should remain distinct.

2.5 No Universal Partner Approval

Approval of one project does not approve future projects.

2.6 No Automatic Continuity

Renewal requires review.

2.7 No Rights Beyond Agreement

Partners receive only the rights explicitly granted.

2.8 No Hidden Authority

Private agreements should not create concealed public-governance authority.

3. Canonical Definitions

Definitions in `TERMINOLOGY.md` govern.

3.1 Partnership

A governed relationship in which two or more parties coordinate resources, expertise, access, activities, or public work toward a defined purpose.

3.2 Partner

An organization or institution party to an approved partnership.

The title should not be used for an ordinary vendor or informal contact unless the relationship warrants it.

3.3 Collaboration

Coordinated activity that may or may not constitute a formal partnership.

3.4 Liaison

A formally recognized communication or participation relationship with defined procedural rights.

3.5 Sponsor

A party providing money, resources, or services in support of an activity.

Sponsorship does not imply technical or editorial authority.

3.6 Funder

A party providing financial support.

3.7 Contractor

A party providing services under contract.

3.8 Vendor

A party selling goods or services.

3.9 Strategic Partner

A partner engaged in a relationship affecting multiple programs, institutional capabilities, public positioning, or long-term strategy.

This term requires enhanced approval.

3.10 Research Partner

A party collaborating on defined research.

3.11 Standards Partner

A party collaborating on standards development, liaison, coordination, implementation, or interoperability.

3.12 Evaluation Partner

A party collaborating on evaluation design, administration, access, review, or infrastructure.

3.13 Public-Interest Partner

A party contributing expertise, representation, affected-party knowledge, rights analysis, accountability, or remedy.

3.14 Government Partner

A public authority or governmental entity engaged in a defined relationship.

The exact authority category should be stated.

3.15 International Partner

A party operating across jurisdictions or established through an international legal or institutional framework.

The term does not imply international recognition of Standards Body.

3.16 Material Partnership

A partnership likely to affect mission, authority, funding, independence, public credibility, standards, evaluations, security, data, intellectual property, international representation, or affected parties.

3.17 Exclusive Partnership

A relationship limiting one or more parties from comparable relationships with others.

3.18 Partnership Due Diligence

The structured assessment of mission, authority, ownership, conduct, conflicts, funding, legal, rights, security, reputation, public claims, and exit risk before and during a relationship.

3.19 Partnership Capture

Improper influence over Standards Body's priorities, methods, governance, findings, standards, evaluation, publication, or public claims through a partnership.

3.20 Partner Claim Drift

Expansion of public claims beyond the agreed relationship.

3.21 Logo Laundering

Use of names, logos, marks, advisors, or institutional association to imply endorsement, approval, authority, or legitimacy beyond the actual relationship.

3.22 Access Dependence

Reliance on a partner for data, systems, infrastructure, funding, or permissions in a manner that can influence independent judgment.

3.23 Joint Work Product

An output created under a defined shared process with allocated authorship, ownership, review, approval, and publication rights.

3.24 Partnership Register

The structured public and internal record of material partnerships.

3.25 Partnership Incident

An event that may materially affect the integrity, legality, safety, independence, reputation, or continuation of a partnership.

4. Partnership Architecture

The Standards Body partnership system contains twelve linked layers.

4.1 Purpose Layer

Defines:

- Public-interest objective
- problem
- expected outcome
- affected parties
- why partnership is necessary
- why unilateral work is insufficient

4.2 Identity Layer

Defines:

- Legal entities

- organizational units
- authorized representatives
- ownership
- affiliates
- applicable jurisdictions

4.3 Relationship Layer

Defines the exact relationship type.

4.4 Authority Layer

Defines:

- Who approved the relationship
- who may bind each party
- which decisions remain independent
- which decisions are joint
- which authority is absent

4.5 Contribution Layer

Defines:

- Funding
- staff
- expertise
- access
- data
- infrastructure
- intellectual property
- communications
- implementation

4.6 Risk Layer

Assesses:

- Conflict
- capture
- human rights
- security
- privacy
- legal
- financial
- reputation

- competition
- continuity

4.7 Agreement Layer

Creates enforceable or documented terms proportionate to the relationship.

4.8 Operating Layer

Defines:

- Governance
- work plan
- milestones
- review
- publication
- incident handling
- change control

4.9 Transparency Layer

Defines what should be published and what may remain protected.

4.10 Monitoring Layer

Tests whether the relationship remains aligned and independent.

4.11 Exit Layer

Defines:

- Suspension
- termination
- records
- data
- intellectual property
- public claims
- continuity
- post-exit obligations

4.12 Historical Layer

Preserves the complete relationship record.

4.13 Architecture Rule

A public announcement is not a partnership framework.

A memorandum is not sufficient if authority, data, funding, publication, or exit remain undefined.

5. Partner Categories

5.1 Government and Public Authorities

- National governments
- regional governments
- local governments
- regulators
- public research institutes
- government laboratories
- procurement bodies
- international public organizations

5.2 Standards Organizations

- International standards organizations
- national standards bodies
- regional standards organizations
- sector standards bodies
- consortia
- open standards communities

5.3 Evaluation and Assurance Institutions

- Evaluation laboratories
- red-team organizations
- inspection bodies
- audit bodies
- certification bodies
- accreditation bodies
- proficiency-testing providers
- peer-evaluation organizations

5.4 AI Developers and Deployers

- Frontier AI laboratories
- model providers
- open-weight developers

- cloud providers
- application developers
- enterprise deployers
- sector-specific operators

5.5 Academic and Research Institutions

- Universities
- research centers
- laboratories
- scholarly societies
- libraries
- archives
- research infrastructures

5.6 Civil Society and Public-Interest Organizations

- Human-rights organizations
- consumer organizations
- labor organizations
- disability organizations
- environmental groups
- community organizations
- public-interest technology groups
- advocacy organizations

5.7 Affected Communities

- Workers
- users
- people subject to automated decisions
- communities exposed to systemic risk
- public-service recipients
- domain professionals
- local and Indigenous communities

5.8 Philanthropic and Funding Institutions

- Foundations
- public grant makers
- research funders
- pooled funds
- donor-advised entities
- mission-aligned investors

5.9 Professional and Technical Communities

- Open-source communities
- professional associations
- technical forums
- practitioner networks
- incident-sharing communities
- security researchers

5.10 Infrastructure and Service Providers

- Cloud providers
- data providers
- secure facilities
- software vendors
- translation providers
- accessibility providers
- legal and accounting services
- communications providers

5.11 Media and Public-Education Organizations

A media organization may collaborate on public education or events.

Editorial independence should remain explicit.

5.12 Mixed Organizations

An organization may occupy several categories.

Review should address each role separately.

6. Relationship Classification

6.1 Informal Exchange

Characteristics:

- Information sharing
- no ongoing commitment
- no funding
- no branding
- no confidential access
- no joint authority

Approval:

- Operational owner

6.2 Consultation

Characteristics:

- Advice or feedback
- no decision rights
- bounded purpose
- possible attribution

Approval:

- Program owner

6.3 Research Collaboration

Characteristics:

- Shared research
- defined methods
- authorship
- data
- publication
- intellectual property

Approval:

- Research authority
- enhanced review when material

6.4 Standards Liaison

Characteristics:

- Formal or informal standards coordination
- defined participation rights
- no implied adoption
- no implied voting rights

Approval:

- Standards authority

6.5 Model or Data Access Relationship

Characteristics:

- Access to systems, weights, interfaces, data, logs, or environments
- confidentiality
- security
- publication risk
- access dependence

Approval:

- Technical, security, and governance review

6.6 Evaluation Collaboration

Characteristics:

- Joint design, administration, review, replication, infrastructure, or protected-task work

Approval:

- Evaluation authority
- independence review

6.7 Funding Relationship

Characteristics:

- Grant
- donation
- sponsorship
- restricted project funding
- in-kind contribution

Approval:

- Funding authority
- conflict review

6.8 Government Advisory Relationship

Characteristics:

- Advice to a public institution
- no delegated authority unless expressly provided
- possible confidentiality and public-record implications

Approval:

- Board or delegated executive, depending on materiality

6.9 Implementation Partnership

Characteristics:

- Pilot
- deployment study
- standards implementation
- training
- capacity building
- regional hub

Approval:

- Program and operational authority

6.10 Strategic Partnership

Characteristics:

- Multi-year
- multi-program
- high public visibility
- significant funding or access
- institutional or authority implications

Approval:

- Governing Board

6.11 Vendor Relationship

Characteristics:

- Service provision
- no public co-ownership
- no institutional status

Approval:

- Procurement authority

A vendor should not be called a partner merely for marketing.

6.12 Exclusive Partnership

Characteristics:

- Limits comparable work
- creates dependency
- may affect competition or participation

Approval:

- Enhanced board review

6.13 Joint Venture or New Entity

Characteristics:

- New legal vehicle
- shared ownership
- shared governance
- liability
- asset contribution
- major authority implications

Approval:

- Constitutional or M4-level review under `VERSION_HISTORY.md`
-

7. Partnership Tiers

Tier P0: Contact

No partnership.

Examples:

- Meeting
- conference exchange
- introduction
- source sharing

Tier P1: Bounded Collaboration

Examples:

- One workshop
- one consultation
- one joint event

- limited expert exchange

Requirements:

- Defined purpose
- owner
- public-claims rules
- basic conflict check

Tier P2: Program Partnership

Examples:

- Research project
- standards liaison
- pilot
- translation program
- regional project

Requirements:

- Written agreement
- due diligence
- conflict review
- publication terms
- data and intellectual-property terms
- monitoring
- exit

Tier P3: Material Strategic Partnership

Examples:

- Multi-year institutional relationship
- major funder
- frontier developer access
- government program
- standards or assurance infrastructure
- regional institutional hub

Requirements:

- Enhanced due diligence
- board approval
- public summary
- annual review
- concentration analysis
- independent monitoring

- termination plan

Tier P4: Authority-Shaping or Entity-Forming Relationship

Examples:

- Delegated public function
- formal regulatory role
- new joint institution
- international recognition arrangement
- exclusive standards or accreditation function
- merger-like structure

Requirements:

- Constitutional review
- legal analysis
- public consultation where appropriate
- independent review
- formal transition
- identity update
- version-history record

7.1 Tier Review

A relationship should be reclassified when its scope, funding, access, duration, branding, or authority changes.

7.2 No Tier Inflation

A high tier is not a prestige label.

It indicates governance burden and consequence.

8. Partnership Authority and Approval

8.1 Governing Board Reserved Matters

The Governing Board should approve:

- P3 and P4 relationships
- exclusive partnerships
- government relationships implying recognition or authority
- partnerships affecting standards independence
- partnerships affecting accreditation or certification

- relationships creating a new entity
- material model-provider relationships
- major restricted funding
- relationships creating significant public-risk exposure
- partnership termination likely to affect institutional continuity

8.2 Executive Authority

The executive may approve:

- P1 and P2 relationships within delegation
- ordinary research collaborations
- routine vendors
- implementation pilots
- nonmaterial liaisons

8.3 Program Authority

Program leaders may propose but should not unilaterally approve a material relationship involving their own funding or access dependence.

8.4 Specialist Review

Required as relevant:

- Legal
- standards
- research
- evaluation
- security
- privacy
- human rights
- finance
- competition
- international
- communications

8.5 Conflict Review

Decision makers with material partner relationships should recuse or receive documented controls.

8.6 Authority Record

Every material approval should identify:

- Decision authority
- delegation
- date
- scope
- conditions
- dissent
- review date
- termination authority

8.7 No Retroactive Approval

Work should not begin before necessary approval except under documented emergency authority.

8.8 Public Approval Claim

A board-approved partnership does not imply board endorsement of the partner generally.

9. Partnership Intake

9.1 Intake Record

Capture:

- Proposed partner
- legal entity
- relationship type
- purpose
- expected contribution
- requested rights
- funding
- data
- intellectual property
- access
- branding
- duration
- geographic scope
- affected parties
- urgency
- proposer

9.2 Identity Verification

Verify:

- Legal name
- registration
- ownership
- governance
- authorized representative
- affiliates
- sanctions status where relevant
- official contact

9.3 Duplicate and Existing Relationship Check

Identify:

- Prior agreements
- active collaborations
- disputes
- funding
- contributor roles
- standards relationships
- public claims
- conflicts

9.4 Preliminary Screening

Screen for:

- Mission fit
- authority inflation
- serious misconduct
- corruption
- human-rights risk
- security risk
- illegal purpose
- severe conflict
- unmanageable exclusivity

9.5 Intake Outcome

- Proceed
- proceed with conditions
- request information
- escalate

- defer
- decline
- prohibit

9.6 No Relationship by Announcement

A relationship should not be announced before approval and agreement.

10. Partnership Due Diligence

10.1 Proportionality

Due diligence should scale with:

- Tier
- funding
- duration
- authority
- data
- security
- public visibility
- dependence
- affected-party risk
- jurisdiction
- exclusivity

10.2 Core Review Domains

Identity and Ownership

- Legal entity
- beneficial ownership
- affiliates
- control
- governance

Mission and Conduct

- Stated mission
- actual activity
- public record
- controversies
- corrections
- accountability

Authority

- Legal mandate
- regulatory role
- standards role
- accreditation role
- certification role
- ability to bind

Financial

- Funding
- solvency
- concentration
- restrictions
- conflicts
- sustainability

Human Rights

- Actual and potential impacts
- affected communities
- remedy
- retaliation
- defenders
- labor
- discrimination

Technical

- Competence
- methods
- security
- system access
- claims
- incidents
- quality

Legal and Regulatory

- Compliance
- sanctions
- export controls
- litigation
- enforcement
- procurement restrictions
- competition

Security and Privacy

- Information security
- data governance
- breach history
- access
- vendors
- jurisdiction

Public Claims

- Marketing
- logos
- authority statements
- correction history
- representation

Exit

- Dependency
- records
- data
- continuity
- public communication
- post-exit restrictions

10.3 Evidence Sources

Use:

- Official records
- audited financials where available
- policies
- public filings
- legal decisions
- regulatory records
- independent reporting
- references
- technical evidence
- interviews
- direct disclosure

10.4 Adverse Information

Adverse information should be:

- Verified

- contextualized
- assessed for severity
- connected to the proposed relationship
- reviewed for correction
- disclosed to decision makers

10.5 No Reputation Shortcut

Prestige does not replace due diligence.

10.6 No Category Presumption

Government, nonprofit, academic, industry, and civil-society status do not establish trust automatically.

10.7 Partner Response

The proposed partner may respond to material concerns.

10.8 Due-Diligence Outcome

- Approved
- approved with conditions
- enhanced monitoring
- limited scope
- independent oversight
- deferred
- declined
- prohibited

10.9 Review Date

Material due diligence should be refreshed during the relationship.

11. Mission and Public-Interest Fit

11.1 Mission Test

The relationship should advance one or more legitimate functions:

- Research
- evidence
- standards

- evaluation
- assurance
- interoperability
- capacity
- public understanding
- affected-party participation
- institutional development

11.2 Necessity Test

Ask:

- Why is this partner needed?
- Is another arrangement safer?
- Can the work be performed independently?
- Does the partner control an essential resource?
- Is dependence temporary or structural?

11.3 Public-Benefit Test

Identify:

- Beneficiaries
- expected benefit
- distribution
- risk
- public output
- access
- accountability

11.4 Mission Drift

Reject or narrow relationships that primarily advance:

- Marketing
- partner legitimacy
- private market advantage
- political prestige
- product launch
- exclusive access
- revenue unrelated to mission

11.5 Institutional Capacity

A valuable relationship may still be declined if Standards Body lacks capacity to govern it.

11.6 Opportunity Cost

Consider what the partnership displaces.

11.7 Reassessment

Mission fit should be reviewed after material change.

12. Human Rights and Affected-Party Due Diligence

12.1 Human-Rights Baseline

The UN Guiding Principles on Business and Human Rights distinguish state duties, organizational responsibility to respect rights, and access to remedy.[^ungp]

Standards Body should use that architecture as a minimum partnership lens.

12.2 Impact Relationships

Assess whether Standards Body may:

- Cause adverse impact
- contribute to adverse impact
- become directly linked through a partner relationship

12.3 Salience

Prioritize severe risks based on:

- Scale
- scope
- irremediability
- likelihood
- vulnerability
- time sensitivity

12.4 Affected-Party Engagement

Meaningful engagement should be:

- Timely
- accessible
- safe
- informed
- culturally competent

- nonretaliatory
- capable of changing the decision

12.5 Human-Rights Defenders

Review whether the relationship may expose or silence:

- Researchers
- whistleblowers
- workers
- journalists
- community advocates
- civil-society participants

OHCHR guidance emphasizes the role of human-rights defenders in due diligence and understanding affected-stakeholder concerns.[^hrd-guidance]

12.6 Remedy

The agreement should not prevent:

- Complaint
- correction
- lawful disclosure
- investigation
- remediation
- access to external remedy

12.7 Severe Harm

A relationship should not proceed unchanged where severe harm cannot be prevented or mitigated credibly.

12.8 Public-Interest Dissent

Partners should not condition access or funding on silence concerning legitimate public-interest criticism.

12.9 Vulnerable and Marginalized Groups

Review differential impacts.

12.10 Rights Record

Document:

- Risks
 - affected groups
 - engagement
 - controls
 - unresolved harm
 - monitoring
 - remedy
 - decision
-

13. Independence and Capture Controls

13.1 Independence Dimensions

Assess:

- Governance independence
- financial independence
- methodological independence
- informational independence
- operational independence
- publication independence
- personnel independence
- security independence
- political independence

13.2 Capture Pathways

A partner may influence Standards Body through:

- Funding
- privileged access
- employment
- board appointments
- standards participation
- data control
- infrastructure
- legal pressure
- public endorsement
- future contracts
- media access
- exclusive technical knowledge

- withdrawal threats

13.3 Dependency Register

Material dependencies should identify:

- Resource
- partner
- duration
- alternatives
- switching cost
- effect of withdrawal
- mitigation
- owner
- review date

13.4 Diversification

Standards Body should avoid material dependence on one:

- Developer
- government
- funder
- evaluator
- cloud provider
- region
- standards organization
- data source
- intellectual tradition

13.5 Independent Workstream Control

Partnership-funded work should preserve:

- Research question integrity
- method choice
- evidence standards
- reviewer independence
- publication rights
- correction authority
- dissent

13.6 Access Leverage

An access provider should not condition unrelated access on favorable treatment.

13.7 Governance Seat

A partner should not receive a governing seat solely because it contributes money, systems, or prestige.

13.8 Veto

No partner should receive a permanent veto over:

- Standards
- findings
- publication
- correction
- complaints
- termination
- institutional identity

13.9 Capture Response

Controls may include:

- Recusal
- independent reviewer
- parallel evidence pathway
- scope reduction
- funding diversification
- public disclosure
- alternative provider
- suspension
- termination

13.10 Capture Audit

P3 and P4 relationships should receive periodic capture review.

14. Conflicts of Interest

14.1 Conflict Categories

- Financial
- ownership
- governance
- employment
- consulting

- research
- intellectual
- personal
- political
- legal
- competitive
- future opportunity
- access
- publication
- reputational

14.2 Institutional Conflict

A conflict may exist even when no individual is personally conflicted.

14.3 Partner Disclosure

A material partner should disclose relevant:

- Ownership
- funders
- clients
- affiliates
- litigation
- regulatory matters
- standards interests
- evaluator interests
- product interests
- lobbying
- political roles

subject to lawful limits.

14.4 Standards Conflict

A party benefiting from a requirement should not control the requirement's development.

Participation may remain appropriate with balance, disclosure, consensus protections, and public review.

14.5 Evaluation Conflict

A developer should not control an independent evaluation of its own system.

14.6 Funding Conflict

A funder should not control findings.

14.7 Government Conflict

A government may have legitimate policy authority and political interests.

Both should be visible.

14.8 Civil-Society Conflict

Advocacy commitments should be disclosed without treating advocacy as disqualifying automatically.

14.9 Conflict Controls

- Disclosure
- recusal
- balanced representation
- independent review
- separate decision authority
- method preregistration
- public comment
- audit
- publication of dissent
- refusal

14.10 Unmanageable Conflict

The relationship should not proceed where controls cannot preserve credible independence.

15. Funding and Resource Contributions

15.1 Funding Purpose

Funding should support defined public-interest work.

15.2 Funding Types

- Unrestricted support
- restricted grant
- project contract

- sponsorship
- in-kind contribution
- secondment
- compute credit
- data access
- model access
- event support
- pooled fund

15.3 Funding Record

Record:

- Funder
- amount or value
- purpose
- restrictions
- duration
- payment schedule
- reporting
- publication rights
- ownership
- refund
- termination
- conflicts

15.4 Prohibited Funding Conditions

- Predetermined conclusion
- favorable standard
- favorable evaluation
- publication veto
- concealed attribution
- retaliation
- permanent governance right
- preferential complaint outcome
- unsupported endorsement
- exclusive regulator access

15.5 Funder Concentration

Apply the institutional concentration limits in `INSTITUTION_DESIGN.md` and `GOVERNANCE_FRAMEWORK.md`.

15.6 In-Kind Valuation

Estimate the fair value and dependence created by:

- Compute
- software
- data
- staff
- facilities
- travel
- legal services
- communications
- model access

15.7 Restricted Funding

Restricted funding should not create hidden control of the institutional research agenda.

15.8 Unspent Funds

Define treatment after completion or termination.

15.9 Financial Reporting

Publish material funding at the level required by `TRANSPARENCY_FRAMEWORK.md`.

15.10 Funding Exit

Standards Body should maintain enough operational resilience to reject improper influence.

16. Government and Public-Authority Relationships

16.1 Relationship Classification

State whether the government relationship is:

- Consultation
- advisory
- research
- grant
- contract
- procurement
- pilot
- standards coordination

- recognized role
- delegated function
- regulatory function
- enforcement support

16.2 Authority Source

Identify:

- Statute
- regulation
- executive authority
- contract
- memorandum
- procurement
- informal request
- no legal authority

16.3 No Authority Inflation

Do not use:

- Government-backed
- official partner
- regulator-approved
- designated standards body
- public authority

unless the precise basis supports the claim.

16.4 Government Direction

A government may define lawful contractual objectives.

It should not covertly control independent research conclusions or standards consensus.

16.5 Public Records

Government partnerships may create:

- Public-record obligations
- procurement disclosures
- audit
- lobbying rules
- records retention
- national-security controls

- accessibility duties

16.6 Political Neutrality

Standards Body should cooperate across lawful administrations without becoming a partisan instrument.

16.7 Law Enforcement and Security Agencies

Enhanced review should address:

- Legal basis
- human rights
- surveillance
- secrecy
- dual use
- affected parties
- remedy
- publication
- mission fit

16.8 Government Funding

Disclose:

- Agency
- program
- amount
- restrictions
- deliverables
- publication rights
- political or legal conditions

16.9 Delegated Function

A delegated function requires:

- Valid legal basis
- clear scope
- governance
- competence
- accountability
- appeal
- public notice
- identity update
- version-history record

16.10 International Government Cooperation

Avoid implying representation of governments not party to the relationship.

17. Standards-Organization Relationships

17.1 Purpose

Standards cooperation should reduce duplication, improve coherence, and enable interoperability.

17.2 Relationship Types

- Informal coordination
- liaison
- joint working group
- technical contribution
- standards adoption
- referencing
- implementation mapping
- joint publication
- secretariat support

17.3 Procedural Rights

State whether Standards Body may:

- Attend
- submit documents
- nominate experts
- participate in working groups
- comment
- vote
- observe
- receive documents
- publish liaison reports

17.4 ISO and IEC Liaisons

The ISO/IEC Directives establish formal categories and criteria for liaison participation.[^iso-directives]

A liaison should be described by its actual category and rights.

17.5 WTO Principles

Standards partnerships should support:

- Transparency
- openness
- impartiality and consensus
- effectiveness and relevance
- coherence
- development dimension^[^wto-six]

17.6 No Standards-Status Inflation

A joint project does not make its output an international standard.

17.7 Coherence Review

Before launching work, identify:

- Existing standards
- active projects
- national work
- regional work
- consortia
- potential conflict
- opportunity for liaison

17.8 Normative References

Partnership agreements should not force proprietary or inaccessible references without justification.

17.9 Joint Standards Work

Define:

- Lead body
- process
- voting
- public review
- copyright
- publication
- maintenance
- appeals
- withdrawal
- legal status

17.10 Competition

Standards collaboration should avoid exclusionary agreements and anticompetitive conduct.

18. Evaluator, Certification, and Accreditation Relationships

18.1 Evaluator Relationship

Possible purposes:

- Method development
- pilot evaluation
- replication
- proficiency testing
- secure infrastructure
- independent review
- assessor training

18.2 Independence

An evaluator partner should not control Standards Body criteria that determine its own market status.

18.3 Accreditation Relationship

A relationship with an accreditation body may support:

- Criteria mapping
- readiness pilots
- assessor competence
- scheme development
- international recognition analysis

It does not make Standards Body an accreditation body.

18.4 Certification Relationship

A certification-body partnership should define:

- Scheme
- object
- decision authority
- evaluation evidence

- conflicts
- marks
- public claims

18.5 Market Advantage

Standards Body should avoid giving one evaluator exclusive early access to criteria without a public-interest reason and fair pathway.

18.6 Pilot Participation

Pilot status should not imply accreditation or certification.

18.7 Result Independence

Evaluator partners should preserve the ability to issue adverse findings.

18.8 Shared Methods

Define:

- Ownership
- licensing
- validation
- changes
- publication
- security
- commercial use

18.9 Registry

Material assurance relationships should appear in the partnership register.

18.10 Role Separation

Standards Body should not simultaneously:

- Develop exclusive criteria
- sell evaluation
- accredit the evaluator
- certify the client
- decide appeals

without independent institutional separation.

19. AI Developer and Model-Provider Relationships

19.1 Enhanced Risk

Developer relationships can create unusually high dependence because the developer may control:

- Model access
- system information
- logs
- privileged interfaces
- weights
- safeguards
- publication timing
- repeat access
- funding
- technical staff

19.2 Required Agreement Fields

- Legal entity
- system and version
- access mode
- duration
- rate limits
- tools
- safeguards
- logs
- data
- security
- publication
- factual review
- findings
- corrections
- termination
- post-access verification

19.3 Evaluation Independence

The developer may not control:

- Task design where independence is claimed
- scoring
- threshold interpretation
- reviewer selection
- final conclusions

- publication solely due to unfavorable findings

19.4 Factual Review

A developer may review:

- System identity
- technical factual errors
- confidential information
- security-sensitive details
- legal restrictions

Factual review should have:

- Defined duration
- no silence-based veto
- recorded comments
- independent disposition

19.5 Access Withdrawal

The agreement should state:

- Grounds
- notice
- immediate-risk exception
- effect on current work
- publication
- records
- re-evaluation
- public disclosure

19.6 Unrelated Access Leverage

A developer should not condition unrelated access on favorable treatment in another project.

19.7 Product Launch Timing

Standards Body should not coordinate findings primarily to support a launch.

Legitimate security embargo may be used.

19.8 Marketing

The developer may not use the relationship to imply:

- Approval

- certification
- safety
- regulatory recognition
- endorsement
- successful independent evaluation

unless exact evidence supports the claim.

19.9 Developer Funding

Funding and access should be disclosed together.

19.10 Multiple Developers

Where feasible, work across several developers to reduce dependence and improve comparative validity.

19.11 Open-Weight Developer

Review:

- Weight license
- distribution
- fine-tuning
- downstream control
- version identity
- community governance
- safeguard claims

19.12 Deployment Partner

A deployer relationship should address real-world monitoring, incident evidence, user impact, and correction.

20. Academic and Research Partnerships

20.1 Strengths

Academic partners may provide:

- Expertise
- peer review
- laboratories
- students

- archives
- research ethics
- disciplinary breadth

20.2 Risks

- Short-term grants
- personnel turnover
- publication pressure
- prestige incentives
- institutional ownership
- weak operational continuity
- student vulnerability
- conflicts with sponsors
- slow contracting

20.3 Research Governance

Define:

- Protocol
- ethics
- data
- authorship
- preregistration
- publication
- review
- correction
- participant protection
- security

20.4 Students and Trainees

Protect:

- Consent
- supervision
- compensation
- credit
- academic freedom
- whistleblowing
- career interests
- security

20.5 Academic Freedom

The relationship should preserve lawful scholarly criticism.

20.6 Institutional Review

Human-participant and sensitive research should receive appropriate ethics review.

20.7 Publication Timing

Avoid indefinite delay.

20.8 University Branding

Use of a university name should not imply institutional endorsement unless authorized.

20.9 Intellectual Property

University policies should be reviewed before work begins.

20.10 Continuity

Plan for:

- Principal investigator departure
- student graduation
- grant end
- laboratory closure
- record custody

21. Civil-Society and Affected-Community Partnerships

21.1 Purpose

These relationships should improve:

- Rights analysis
- lived-experience evidence
- public accountability
- accessibility
- remedy
- legitimacy
- implementation

21.2 No Symbolic Inclusion

A partner should have meaningful influence appropriate to the work.

21.3 Representation

An organization should not be treated as representing every member of a community without a mandate.

21.4 Compensation

Budget for:

- Time
- preparation
- accessibility
- translation
- travel
- childcare
- technical support
- security

21.5 Power Imbalance

Standards Body should not require communities to disclose sensitive information merely to be heard.

21.6 Safety

Protect participants from:

- Retaliation
- harassment
- exposure
- employment harm
- legal risk
- online abuse

21.7 Evidence Status

Lived experience should be represented accurately under EVIDENCE_STANDARDS.md.

21.8 Advocacy Independence

A civil-society partner should remain free to criticize Standards Body.

21.9 Public Claims

Do not imply community endorsement from participation.

21.10 Remedy

Provide complaint and correction routes.

22. International and Regional Partnerships

22.1 Purpose

International cooperation should support:

- Interoperability
- local relevance
- regional competence
- multilingual work
- cross-border evidence
- capacity
- mutual learning

22.2 No Global Representation Claim

A small group of international partners does not constitute global consensus.

22.3 Regional Authority

Identify whether the partner is:

- Governmental
- intergovernmental
- standards
- academic
- civil society
- industry
- regional network

22.4 Local Expertise

International work should include:

- Local law
- language

- institutions
- culture
- infrastructure
- affected parties
- implementation conditions

22.5 Development Dimension

Partnership design should address participation and capacity constraints consistent with the WTO development principle for international standards.[^wto-six]

22.6 Resource Equity

Avoid extracting data or expertise without durable local benefit.

22.7 Regional Hub

A hub agreement should define:

- Legal entity
- authority
- territory
- brand
- funding
- governance
- standards status
- records
- exit

22.8 Translation

Translated work should follow `VERSION_HISTORY.md` and `WEBSITE_SOURCE_OF_TRUTH.md`.

22.9 Cross-Border Data

Address:

- Legal transfer
- localization
- security
- access
- government demand
- retention
- redress

22.10 Recognition

Do not imply formal mutual recognition without an actual arrangement.

23. Philanthropic and Funder Partnerships

23.1 Due Diligence

Review:

- Source of funds
- governance
- donor restrictions
- political interests
- portfolio conflicts
- reputation
- concentration
- duration
- exit

23.2 Donor Direction

A donor may define a broad supported purpose.

It should not determine findings or standards outcomes.

23.3 Donor-Advised and Anonymous Funding

Anonymous funding requires enhanced review.

The responsible internal body should know enough to assess conflicts and legality.

23.4 Naming Rights

Naming rights should not create authority or permanent influence.

23.5 Restricted Agenda

Avoid funding structures that make neglected topics impossible to pursue.

23.6 Funder Collaboration

A funder may support convening and learning.

It should not participate in technical decisions merely because it funded the work.

23.7 Public Disclosure

Publish material support and restrictions.

23.8 Exit

Plan for funding end without suppressing corrections or unfinished public obligations.

24. Open-Source and Technical-Community Partnerships

24.1 Value

Open communities may provide:

- Code
- methods
- tasks
- review
- replication
- incident discovery
- global participation

24.2 Legal Identity

A community may lack a legal entity.

The agreement should identify accountable maintainers or a fiscal host where needed.

24.3 Contribution Governance

Use:

- License
- contributor agreement where necessary
- code review
- security policy
- maintainers
- version control
- provenance
- conduct

24.4 Open and Protected Work

Open methods may coexist with protected tasks and credentials.

24.5 Maintainer Capture

Monitor concentration of merge, release, and security authority.

24.6 Forking

Licenses and governance should define whether and how work may be forked.

24.7 Community Credit

Provide accurate contribution records.

24.8 Sustainability

Plan for maintenance, funding, succession, and archive.

24.9 No Community Endorsement Claim

A repository contribution does not establish endorsement by all contributors.

25. Vendors, Contractors, and Infrastructure Providers

25.1 Vendor Versus Partner

Use vendor terminology when the relationship is primarily procurement.

25.2 Material Vendor Review

Enhanced review applies when the vendor controls:

- Domain
- cloud
- identity
- data
- security
- communications
- publication
- source repository
- critical compute

- model access

25.3 Contract Requirements

- Service
- performance
- security
- privacy
- incident notice
- subcontracting
- data return
- deletion
- audit
- continuity
- exit
- ownership
- portability

25.4 Vendor Branding

A vendor should not be presented as an institutional partner merely because it provides services.

25.5 Lock-In

Maintain:

- Export
- migration
- backup
- alternate providers
- documentation
- credentials
- institutional accounts

25.6 AI Service Providers

Do not submit protected information to unauthorized external AI services.

25.7 Critical Supplier Incident

A supplier failure should trigger continuity and status review.

26. Joint Research and Evidence Production

26.1 Research Question

The partnership agreement should identify who may:

- Propose the question
- refine scope
- approve the protocol
- select methods
- access data
- interpret results
- approve publication
- correct errors

26.2 Research Independence

A partner may contribute expertise and evidence.

It should not control the result merely because it provided:

- Funding
- data
- systems
- personnel
- infrastructure
- access
- publication support

26.3 Protocol

Material joint research should use a protocol proportionate to consequence.

26.4 Registration

Use preregistration or internal registration where appropriate.

26.5 Source Disclosure

Identify:

- Partner-provided sources
- independently obtained sources
- protected evidence
- contrary evidence

- source restrictions

26.6 Methods

State whether methods are:

- Standards Body methods
- partner methods
- jointly developed
- independently reviewed
- experimental
- validated

26.7 Data Analysis

Preserve independent access to the analysis necessary to verify conclusions.

26.8 Review Rights

Partner review should distinguish:

- Factual review
- security review
- confidentiality review
- methodological review
- editorial comment
- approval right

26.9 Disagreement

The agreement should permit:

- Separate interpretation
- dissenting note
- separate publication
- correction request
- withdrawal of name without erasing evidence

26.10 Research Misconduct

Define reporting, investigation, correction, and publication consequences.

26.11 Joint Conclusions

A joint conclusion should identify which parties approved it.

26.12 Independent Conclusion

Standards Body should be able to state its own supported conclusion when the partner disagrees.

27. Standards and Technical Work Products

27.1 Work-Product Classification

Joint technical work may produce:

- Research report
- technical specification
- implementation guide
- standards proposal
- reference architecture
- crosswalk
- terminology
- test method
- open-source tool
- public comment

27.2 Process Control

The agreement should identify:

- Controlling process
- consensus rules
- voting
- public review
- appeals
- maintenance
- publication
- copyright
- status

27.3 No Private Standard by Partnership Label

A bilateral agreement should not be represented as broad consensus.

27.4 Joint Working Groups

Define:

- Terms of reference

- membership
- chair
- secretariat
- balance
- conflicts
- records
- decisions
- public output
- dissolution

27.5 Normative Authority

A partner should not receive authority to alter a Standard Body requirement outside the approved standards process.

27.6 Implementation Evidence

Partners may provide pilots and feedback.

Their commercial preference should not substitute for general evidence.

27.7 Maintenance

Joint outputs require:

- Owner
- versioning
- source register
- correction
- review date
- retirement
- archive

27.8 Adoption

Each party should state whether it:

- Contributed
- approved
- adopted
- referenced
- implemented
- recognized
- did not endorse

28. Evaluation and Model-Access Partnerships

28.1 Evaluated Object

The agreement should identify:

- Developer
- model
- system
- version
- configuration
- tools
- access mode
- safeguards
- deployment context
- date

28.2 Access Equality

Where comparative claims are made, access conditions should be sufficiently comparable.

28.3 Access Record

Preserve:

- Credentials
- rate limits
- time window
- privileged information
- system changes
- interruptions
- restrictions
- provider intervention

28.4 Task Independence

Protected task design and custody should remain governed independently.

28.5 Safety Controls

Define:

- Stop conditions
- escalation
- information-hazard review

- incident response
- human oversight
- disclosure

28.6 Publication Embargo

An embargo may protect:

- Vulnerability remediation
- task security
- participant safety
- lawful market-sensitive information

It should have:

- Defined purpose
- maximum duration
- release condition
- independent review
- no indefinite suppression

28.7 Adverse Findings

The agreement should define handling without requiring favorable results.

28.8 Re-Evaluation

Access should permit correction or re-evaluation where a material error is identified.

28.9 Provider Response

Publish or preserve the provider's response separately from the independent result.

28.10 Result Use

The partner may not quote results outside scope or omit limitations.

29. Data Governance

29.1 Data Inventory

Identify:

- Data

- owner
- source
- purpose
- rights
- personal information
- sensitivity
- location
- retention
- deletion
- sharing

29.2 Purpose Limitation

Use data only for approved purposes.

29.3 Data Minimization

Collect and share only what is necessary.

29.4 Provenance

Preserve:

- Origin
- collection
- transformations
- labels
- versions
- corrections
- access

29.5 Data Quality

Define:

- Validation
- missingness
- bias
- representativeness
- update
- correction

29.6 Personal Data

Address:

- Lawful basis
- consent
- notice
- rights
- security
- retention
- transfer
- de-identification
- re-identification risk

29.7 Sensitive and Protected Data

Use enhanced:

- Access control
- secure environment
- logging
- output review
- incident handling
- deletion verification

29.8 Data Controller and Processor Roles

Identify legal roles where applicable.

29.9 Partner Data Rights

A partner should not receive rights beyond the agreement.

29.10 Data Return and Deletion

Define after:

- Project completion
- termination
- withdrawal
- legal request
- incident

29.11 Derived Data

Define ownership and use of:

- Annotations
- features
- scores
- analyses
- embeddings
- synthetic data
- aggregate results

29.12 Data Audit

Material data partnerships should permit verification of compliance.

30. Intellectual Property and Licensing

30.1 Intellectual-Property Inventory

Identify:

- Pre-existing work
- joint work
- code
- data
- methods
- trademarks
- patents
- confidential know-how
- publications
- translations
- task assets

30.2 Background Intellectual Property

Each party retains its background intellectual property unless the agreement states otherwise.

30.3 Foreground Intellectual Property

Define ownership of work created through the partnership.

30.4 Public-Interest Licensing

Prefer licenses that support:

- Inspection
- implementation
- correction
- research
- interoperability
- long-term access

subject to security and rights constraints.

30.5 Open Standards

Normative requirements should not depend unnecessarily on inaccessible proprietary rights.

30.6 Patent Disclosure

Standards-related partnerships should require timely disclosure of relevant patent interests according to the controlling standards process.

30.7 Code Licensing

Define:

- License
- dependencies
- contribution
- patents
- security
- maintenance
- fork
- archive

30.8 Data Licensing

Data rights may differ from code and documentation rights.

30.9 Trademark

Use of names, logos, marks, and certification-like symbols should be separately licensed and controlled.

30.10 Post-Termination Rights

Define continued use of:

- Published outputs
- licenses
- citations
- archives
- confidential material
- marks

30.11 Moral Rights and Attribution

Respect applicable authorship and attribution rights.

30.12 Intellectual-Property Dispute

A rights dispute should not justify false public claims or destruction of institutional history.

31. Publication Rights and Editorial Independence

31.1 Publication Baseline

Standards Body should preserve the right to publish accurate, evidence-based work within lawful security, privacy, confidentiality, and intellectual-property limits.

31.2 Review Period

Partner review should have a defined period.

31.3 Permitted Review Purposes

- Correct factual error
- identify confidential information
- identify security risk
- identify legal restriction
- provide response
- identify partner attribution issue

31.4 Impermissible Control

A partner should not:

- Rewrite supported conclusions

- remove unfavorable findings
- require promotional language
- delay indefinitely
- select only favorable results
- prohibit correction
- require false equivalence
- conceal funding or conflict

31.5 Publication Delay

A limited delay may be justified for:

- Security remediation
- patent filing
- participant safety
- legal compliance
- coordinated incident disclosure

31.6 Publication Veto

A material partner veto is presumptively unacceptable for public-interest research.

Any exception requires:

- Legal basis
- narrow scope
- maximum duration
- independent review
- public disclosure where possible

31.7 Partner Response

A partner may publish a response.

31.8 Joint Publication

Identify:

- Authors
- contributors
- institutional approvals
- conclusions
- dissent
- source status
- corrections

31.9 Withdrawal of Name

A partner may withdraw its name from a joint publication before release, subject to attribution and record rules.

It should not erase completed work or evidence.

31.10 Correction Rights

Standards Body retains authority to correct its publication.

31.11 Publication After Exit

Termination should not automatically prevent publication of completed lawful work.

32. Confidentiality

32.1 Confidentiality Purpose

Protect legitimate interests without concealing invalidity, misconduct, or public-risk information improperly.

32.2 Confidential Information

May include:

- Trade secrets
- protected evaluation tasks
- system information
- personal data
- security findings
- unreleased research
- legal advice
- contract terms
- incident evidence

32.3 Classification

Apply the information classes in `TRANSPARENCY_FRAMEWORK.md`.

32.4 Need to Know

Access should be based on role and purpose.

32.5 Confidentiality Duration

Define duration and review.

32.6 Exceptions

Permit disclosure where lawfully required for:

- Legal obligation
- court order
- regulatory reporting
- serious danger
- protected whistleblowing
- correction
- independent review

subject to applicable process.

32.7 Residual Knowledge

Avoid broad clauses that permit unrestricted use of protected knowledge through memory.

32.8 Confidentiality and Publication

Redact or aggregate where possible rather than suppressing entire findings.

32.9 Return and Destruction

Define post-exit handling.

32.10 Breach

A breach should trigger:

- Containment
 - notice
 - investigation
 - correction
 - status review
 - possible termination
-

33. Security

33.1 Security Review

Required when the partnership involves:

- Frontier systems
- model weights
- privileged access
- held-out tasks
- vulnerabilities
- dangerous capabilities
- critical infrastructure
- personal data
- confidential government information
- production credentials

33.2 Security Responsibilities

Allocate:

- Risk assessment
- access approval
- identity
- logging
- encryption
- storage
- devices
- networks
- physical security
- incident response
- recovery
- reporting

33.3 Shared Environment

Define:

- Administrator
- access
- data
- logs
- changes
- backups
- deletion

- monitoring
- jurisdiction

33.4 Personnel Security

Address:

- Authorization
- screening where lawful
- training
- confidentiality
- least privilege
- departure

33.5 Supply Chain

Review subcontractors and technical dependencies.

33.6 Security Incident

Define:

- Notification time
- contact
- evidence preservation
- coordination
- public disclosure
- regulator notice
- remediation
- continuation

33.7 Security Review Rights

Standards Body should be able to verify material controls directly or through qualified independent evidence.

33.8 No Security Pretext

Security should not be invoked broadly to suppress criticism or conceal conflicts.

33.9 Dangerous Information

Publication should follow information-hazard review.

33.10 Security Exit

Revoke:

- Credentials
- keys
- access
- devices
- shared accounts
- permissions
- certificates

promptly after exit.

34. Branding, Names, Logos, and Marks

34.1 Branding Principle

Brand use should describe the relationship, not manufacture authority.

34.2 Approval

Use of Standards Body's:

- Name
- logo
- domain
- publication design
- seals
- badges
- marks

requires written approval.

34.3 Permitted Relationship Language

Examples:

- Research collaborator on [project]
- Funding supporter of [project]
- Participant in [pilot]
- Standards liaison for [defined process]
- Model-access provider for [evaluation]
- Regional convening collaborator

34.4 Prohibited Language

Without exact basis:

- Official partner
- certified by Standards Body
- accredited by Standards Body
- approved by Standards Body
- global standards authority partner
- government-recognized through Standards Body
- Standards Body safe AI partner
- endorsed technology

34.5 Partner Logo

A logo may be displayed only with:

- Relationship label
- scope
- duration
- no-endorsement context
- current status

34.6 Logo Placement

Design should not imply:

- Equal authority
- joint ownership
- certification
- public approval
- government recognition

34.7 Marks and Certification-Like Badges

Standards Body should not issue partnership badges that resemble certification or accreditation marks.

34.8 Partner Materials

The partner should submit material uses for review.

34.9 Digital Monitoring

Monitor websites, social media, press releases, reports, and sales materials.

34.10 Correction and Takedown

The agreement should require prompt correction.

34.11 Post-Exit Use

Use of name and logo should end except for accurate historical references.

35. Public Communications

35.1 Announcement

A partnership announcement should state:

- Parties
- relationship type
- purpose
- duration
- funding
- work
- authority limits
- no-endorsement note
- contact
- public summary

35.2 Joint Statement

A joint statement should identify whether each statement is:

- Jointly agreed
- attributed to one party
- background
- future intention
- current fact

35.3 Spokespersons

Only authorized persons may speak for the relationship.

35.4 Media Inquiries

Coordinate facts without requiring identical opinions.

35.5 Press Release Approval

Approval should cover factual relationship description.

It should not create partner control over unrelated Standards Body speech.

35.6 Social Media

Social posts should preserve authority limits.

35.7 Crisis Communications

Define lead, coordination, legal review, security, corrections, and public notice.

35.8 Public Disagreement

Partners may disagree publicly.

The relationship should not require artificial consensus.

35.9 Correction

False or outdated announcements should be corrected across channels.

35.10 Historical Record

Preserve original and corrected public statements.

36. Joint Governance and Decision Rights

36.1 Governance Structure

A material project may use:

- Steering committee
- technical committee
- research group
- security group
- public-interest advisory group
- secretariat
- independent review panel

36.2 Terms of Reference

Define:

- Purpose
- membership
- chair
- quorum
- decisions
- conflicts
- records
- escalation
- duration
- dissolution

36.3 Decision Classes

Standards Body Reserved

- Institutional identity
- final Standards Body position
- use of name
- publication of Standards Body work
- correction of Standards Body work
- internal personnel
- internal governance

Partner Reserved

- Partner's internal policy
- partner systems
- partner public position
- partner personnel
- partner legal compliance

Joint

- Shared work plan
- joint budget
- joint event
- jointly authored output
- shared infrastructure
- agreed public announcement

36.4 Deadlock

Define:

- Escalation
- mediation
- independent review
- separate publication
- scope reduction
- termination

36.5 No Joint Veto Over Truth

Joint governance should not prevent either party from correcting its own false statement or complying with law.

36.6 Records

Preserve decisions, dissent, conflicts, and changes.

36.7 Observers

Observer rights should be defined.

36.8 Community Participation

Affected-party participation should not be subordinated automatically to organizational voting power.

37. Partnership Agreement Architecture

37.1 Parties

Identify exact legal entities and authorized signatories.

37.2 Purpose

Define the public-interest purpose and scope.

37.3 Term

Define:

- Start
- end
- renewal
- review
- termination
- survival

37.4 Contributions

Define each party's:

- Money
- staff
- expertise
- access
- data
- infrastructure
- intellectual property
- communications

37.5 Governance

Define decisions and escalation.

37.6 Independence

Preserve technical, editorial, evidence, standards, and governance independence.

37.7 Funding

Define payment, restrictions, reporting, and refund.

37.8 Data and Privacy

Define lawful use and responsibilities.

37.9 Intellectual Property

Define background, foreground, licensing, and archive.

37.10 Publication

Define review, delay, correction, dissent, and response.

37.11 Confidentiality and Security

Define classification, access, incidents, return, and destruction.

37.12 Branding

Define names, logos, marks, and public claims.

37.13 Conduct

Require compliance with:

- Law
- anti-corruption
- competition
- sanctions
- human rights
- nonretaliation
- code of conduct

37.14 Monitoring

Define reporting, audit, milestones, and review.

37.15 Complaints and Incidents

Define routes and cooperation.

37.16 Termination

Define grounds, notice, immediate action, and post-exit duties.

37.17 Dispute Resolution

Define:

- Negotiation
- mediation
- arbitration
- court
- governing law

- public-law limits

37.18 Entire Relationship

Avoid side agreements that alter public-interest controls without approval.

38. Financial Terms and Procurement

38.1 Fair Value

Financial terms should be documented and reasonable.

38.2 Procurement Integrity

Use fair procurement where goods or services are purchased.

38.3 Related Parties

Disclose and review related-party transactions.

38.4 Hidden Subsidy

Record in-kind contributions and below-market access.

38.5 Payment Milestones

Tie payment to completed work, not favorable findings.

38.6 Expenses

Define eligible expenses and documentation.

38.7 Audit

Material partnerships should permit financial verification.

38.8 Tax

Address applicable tax status and reporting.

38.9 Foreign Funding

Review legal, political, sanctions, security, and public-claim implications.

38.10 Contingent Payment

Prohibit payment contingent on standards adoption, accreditation, certification, favorable evaluation, or regulatory outcome.

39. Competition and Antitrust

39.1 Competition Principle

Partnerships should not become mechanisms for unlawful coordination or exclusion.

39.2 Risk Areas

- Pricing
- market allocation
- boycotts
- exclusive dealing
- sensitive commercial information
- standards exclusion
- certification market control
- evaluator allocation
- procurement manipulation
- access discrimination

39.3 Standards Meetings

Use agendas, minutes, competition guidance, and counsel where appropriate.

39.4 Commercially Sensitive Information

Do not share unnecessary:

- Prices
- customers
- future strategy
- capacity
- bids
- wages
- market allocation

39.5 Technical Necessity

A technical requirement should be justified by evidence and public-interest need.

39.6 Essential Access

Review whether exclusive access to:

- Tests
- data
- infrastructure
- certification
- accreditation
- registries

creates unfair barriers.

39.7 Open Participation

Standards processes should provide fair participation consistent with their scope and governance.

39.8 Competition Review

Required for high-impact industry consortia, standards, shared data, and evaluator schemes.

40. Anti-Corruption and Improper Influence

40.1 Prohibition

Partners should not offer, request, authorize, or accept bribery or improper benefit.

40.2 Covered Benefits

- Cash
- gifts
- travel
- hospitality
- jobs
- contracts
- access
- data
- awards
- political support
- research funding

- publication placement
- admissions
- favors

40.3 Public Officials

Enhanced controls apply to public officials and state-owned entities.

40.4 Intermediaries

Review agents, consultants, lobbyists, and local representatives.

40.5 Gifts and Hospitality

Use low thresholds, disclosure, and refusal where influence may be perceived.

40.6 Facilitation Payments

Prohibit except where an immediate threat to health or safety requires protective action, followed by reporting and review.

40.7 Books and Records

Maintain accurate records.

40.8 Reporting

Provide protected reporting.

40.9 Investigation

Cooperate with lawful investigation while protecting due process.

40.10 Termination

Serious corruption may require immediate suspension or termination.

The United Nations Convention against Corruption provides an international anti-corruption reference framework.[^uncac]

41. Sanctions, Export Controls, and Restricted Parties

41.1 Screening

Where legally relevant, screen:

- Parties
- owners
- affiliates
- individuals
- countries
- end users
- end uses

41.2 Controlled Technology

Frontier AI work may involve:

- Advanced compute
- model weights
- cybersecurity tools
- technical data
- dual-use research
- encryption
- critical infrastructure

41.3 Legal Advice

Obtain qualified advice for material cross-border restrictions.

41.4 No Evasion

Do not structure a partnership to evade lawful controls.

41.5 Humanitarian and Research Exceptions

Assess applicable exceptions carefully.

41.6 Status Change

A sanctions or export-control change may require immediate suspension.

41.7 Public Explanation

Disclose the safest accurate reason where possible.

42. Political Activity and Lobbying

42.1 Political Independence

A partnership should not convert Standards Body into a vehicle for partisan campaigning.

42.2 Policy Engagement

Standards Body may:

- Provide evidence
- comment on policy
- explain standards
- advise institutions
- participate in consultations

within its identity and legal limits.

42.3 Lobbying Disclosure

Identify material lobbying activity conducted jointly or on behalf of the partnership.

42.4 No Implied Government Position

A public official's participation does not imply government endorsement.

42.5 Election Activity

Avoid use of partnership resources for prohibited or inappropriate electoral activity.

42.6 Policy Disagreement

Partners should remain free to hold different policy positions.

43. Environmental and Resource Considerations

43.1 Environmental Review

Assess material partnership effects involving:

- Compute
- energy
- water
- hardware
- travel
- data centers
- electronic waste
- infrastructure

43.2 Resource Contributions

Disclose significant compute or infrastructure contributions.

43.3 Environmental Claims

Do not make unsupported sustainability claims.

43.4 Tradeoffs

Public-interest review should consider environmental cost alongside technical benefit.

43.5 Local Impact

Engage communities affected by infrastructure where material.

44. Accessibility, Language, and Participation

44.1 Accessibility

Partnership activities should provide reasonable accessibility for:

- Meetings
- documents
- websites
- public comments
- events
- tools

- reports

44.2 Language

Provide translation or interpretation proportionate to participation needs.

44.3 Participation Cost

Budget for meaningful participation.

44.4 Time Zones and Geography

Avoid processes that systematically exclude regions.

44.5 Digital Access

Provide lower-bandwidth or asynchronous options where feasible.

44.6 Technical Barriers

Plain-language and technical versions may be needed.

44.7 Participation Record

Track who could and could not participate.

44.8 Accessibility Failure

A partnership claiming inclusion should not exclude the people most affected through its operating design.

45. Partnership Transparency

45.1 Public Partnership Register

The public register should include material partnerships.

45.2 Required Public Fields

- Partner legal name
- relationship type
- purpose

- scope
- duration
- funding or in-kind support
- Standards Body owner
- governance
- data relationship
- intellectual-property model
- publication rights
- branding rights
- authority limits
- current status
- review date
- termination date where applicable

45.3 Protected Information

The public register may omit or generalize:

- Security-sensitive details
- protected evaluation tasks
- personal information
- lawful trade secrets
- active vulnerability information
- confidential government information

The reason for protection should be stated at the safest useful level.

45.4 No-Endorsement Statement

Every material entry should state:

This relationship concerns the defined purpose and does not imply approval, certification, accreditation, governmental recognition, or endorsement of all activities or positions of either party.

45.5 Funding Disclosure

Disclose material funding and in-kind contributions.

45.6 Model-Provider Disclosure

Disclose:

- Access provided
- restrictions
- funding

- publication rights
- factual review
- independence controls

45.7 Government Disclosure

State the precise legal or contractual basis.

45.8 Partnership Status

Use:

- Proposed
- under review
- active
- conditional
- suspended
- ending
- terminated
- completed
- archived

45.9 Historical Register

Preserve ended relationships and status history.

45.10 Correction

A public register error should be corrected visibly.

46. Monitoring and Periodic Review

46.1 Monitoring Purpose

Determine whether the partnership remains:

- Mission aligned
- lawful
- independent
- effective
- secure
- financially sustainable
- accurately described
- beneficial to affected parties

- capable of ending safely

46.2 Monitoring Inputs

- Deliverables
- funding
- conflicts
- incidents
- complaints
- public claims
- security
- data handling
- publication
- affected-party feedback
- legal status
- partner conduct
- dependency
- market concentration

46.3 Review Frequency

P1

At completion or after material change.

P2

At least annually or at major milestones.

P3

At least annually, with quarterly risk monitoring.

P4

Continuous governance oversight and formal periodic review.

46.4 Triggered Review

Trigger after:

- Ownership change
- leadership change
- legal investigation
- enforcement
- severe public allegation
- security incident

- human-rights concern
- conflict disclosure
- funding change
- public claim drift
- access withdrawal
- standards-status change
- government transition
- merger
- insolvency

46.5 Partner Reporting

Material partners should report relevant changes promptly.

46.6 Standards Body Monitoring

Standards Body should not rely only on self-reporting.

46.7 Performance Review

Assess whether intended public outcomes were achieved.

46.8 Independence Review

Assess whether dependence increased.

46.9 Renewal Decision

- Renew
- renew with conditions
- narrow
- monitor
- suspend
- complete
- terminate

46.10 Review Record

Preserve evidence, decision, dissent, conditions, and next review.

47. Complaints and Concerns

47.1 Who May Complain

- Partner
- contributor
- employee
- contractor
- affected person
- community
- evaluator
- developer
- funder
- government
- public-interest organization
- member of the public

47.2 Complaint Subjects

- Misleading partnership claim
- conflict
- interference
- discrimination
- retaliation
- data misuse
- security
- corruption
- publication suppression
- human-rights impact
- procurement
- mark misuse
- failure to deliver
- breach of agreement

47.3 Intake

Record:

- Complainant
- concern
- evidence
- urgency
- confidentiality
- retaliation risk
- requested outcome

47.4 Independent Handling

A partnership owner should not control a complaint alleging the owner's misconduct.

47.5 Interim Action

Possible actions:

- Preserve evidence
- pause work
- restrict access
- suspend branding
- protect complainant
- issue warning
- notify authority

47.6 Investigation

Use competent, conflict-screened investigators.

47.7 Outcome

- No finding
- clarification
- correction
- remediation
- enhanced monitoring
- disciplinary action
- suspension
- termination
- external referral

47.8 Complainant Communication

Provide a safe outcome summary.

47.9 Public Reporting

Publish aggregate complaint data and material systemic findings.

47.10 Nonretaliation

Retaliation is itself a serious partnership breach.

48. Whistleblowing and Protected Disclosure

48.1 Protected Topics

- Fraud
- corruption
- fabricated evidence
- hidden conflict
- security failure
- dangerous conduct
- retaliation
- public deception
- unlawful activity
- serious rights harm
- suppression of findings

48.2 Reporting Channels

- Internal protected channel
- independent governance channel
- security channel
- legal channel
- external authority where lawful

48.3 Confidentiality

Protect identity to the extent lawful and possible.

48.4 Partner Agreement

The agreement should not prohibit lawful protected disclosures.

48.5 No Nondisparagement Shield

Nondisparagement clauses should not prevent truthful reporting of serious concerns.

48.6 Investigation

Protect due process while preventing retaliation.

48.7 Remedy

Provide correction, restoration, compensation, referral, or other action within authority.

49. Partnership Incidents

49.1 Incident Types

- Security breach
- data breach
- false public claim
- unauthorized logo use
- result suppression
- corruption
- conflict concealment
- human-rights harm
- sanctions issue
- unlawful conduct
- task compromise
- intellectual-property dispute
- publication dispute
- access retaliation
- partner insolvency
- regulatory action

49.2 Incident Severity

I0: Minor

No material effect on integrity or public reliance.

I1: Significant

Requires correction or operating change.

I2: Serious

May affect independence, security, rights, or published work.

I3: Critical

Requires immediate suspension, external reporting, or termination consideration.

49.3 Incident Response

1. Protect people.
2. contain risk.
3. preserve evidence.
4. notify responsible functions.
5. classify.

6. investigate.
7. correct public records.
8. assess continuation.
9. notify affected parties.
10. preserve lessons.

49.4 Joint Investigation

A partner implicated in the incident should not control the complete investigation.

49.5 External Authority

Notify regulators, law enforcement, data authorities, funders, or accreditation bodies where law or role requires.

49.6 Public Notice

Publish when the incident materially affects:

- Public reliance
- safety
- rights
- security
- partnership status
- published findings
- authority claims

49.7 Status

The partnership register should reflect suspension or termination promptly.

49.8 Post-Incident Review

Assess:

- Cause
- governance
- agreement
- monitoring
- dependence
- culture
- systemic correction

50. Correction of Partnership Claims and Outputs

50.1 Correction Scope

Corrections may affect:

- Partnership register
- press release
- report
- website
- social media
- logo placement
- partner sales material
- joint publication
- funding disclosure
- authority description

50.2 Correction Authority

Each party should correct its own false statements.

Joint statements require coordinated correction without unreasonable delay.

50.3 Partner Refusal

If a partner refuses to correct a materially false claim, Standards Body should:

- Publish its own correction
- revoke branding rights
- suspend the relationship
- consider termination
- preserve evidence

50.4 Propagation

Update:

- Website
- downloadable files
- registry
- metadata
- social previews
- newsletters
- partner pages
- archives
- translations

50.5 Historical Preservation

Preserve the original and correction.

51. Renewal

51.1 Renewal Is a New Decision

A relationship should not renew automatically merely because no incident was reported.

51.2 Renewal Review

Assess:

- Purpose
- outcomes
- mission
- dependence
- conflicts
- funding
- rights
- security
- public claims
- partner conduct
- legal status
- exit alternatives

51.3 Updated Agreement

Update terms after material change.

51.4 Public Notice

Update duration and status.

51.5 Declined Renewal

A completed relationship may end without wrongdoing.

51.6 Transition

Protect continuity and public clarity.

52. Suspension

52.1 Grounds

- Investigation
- security concern
- public claim drift
- unmanageable conflict
- funding issue
- legal change
- rights concern
- failure to deliver
- access retaliation
- serious complaint
- sanctions concern

52.2 Scope

Suspension may apply to:

- Branding
- data access
- publication
- joint governance
- funding
- one project
- entire relationship

52.3 Immediate Suspension

Use when continuation creates material risk.

52.4 Public Status

State suspension at the safest useful level.

52.5 Restoration

Requires evidence, correction, approval, and updated public status.

53. Termination and Exit

53.1 Termination Grounds

- Mission conflict
- interference
- corruption
- serious misconduct
- material rights harm
- security failure
- unlawful activity
- repeated false public claims
- concealment
- retaliation
- insolvency
- authority change
- strategic completion
- mutual agreement

53.2 Notice

Define ordinary notice and immediate termination.

53.3 Exit Plan

Address:

- Active work
- personnel
- funding
- data
- systems
- credentials
- intellectual property
- publication
- confidential information
- records
- branding
- complaints
- corrections
- affected parties

53.4 Joint Work

Determine whether work will:

- Continue
- transfer
- pause
- publish
- archive
- withdraw
- split into separate outputs

53.5 Public Statement

Use accurate, nonretaliatory language.

53.6 Post-Exit Brand Use

Only accurate historical reference remains permitted.

53.7 Data and Access

Return, delete, retain, or transfer according to agreement and law.

53.8 Corrections After Exit

Each party retains responsibility to correct its public record.

53.9 Survival

Possible surviving terms:

- Confidentiality
- security
- intellectual property
- publication
- records
- audit
- correction
- dispute resolution
- nonretaliation

53.10 No Hostage Relationship

A partner should not retain essential records or credentials to obstruct exit.

54. Continuity, Transfer, and Partner Failure

54.1 Failure Scenarios

- Insolvency
- merger
- acquisition
- closure
- sanctions
- cyber compromise
- government dissolution
- loss of recognition
- loss of key personnel
- infrastructure failure

54.2 Change of Control

A material change in ownership should trigger review.

54.3 No Automatic Transfer

A partnership should not transfer automatically to a materially different entity without approval.

54.4 Record Custody

Define who preserves:

- Agreements
- research
- evidence
- publications
- complaints
- incidents
- corrections
- source code
- data

54.5 Successor

A successor should meet due-diligence and agreement requirements.

54.6 Public Continuity

Update the register and public claims.

54.7 Critical Infrastructure

Maintain alternative access and migration plans.

55. Partnership Metrics

55.1 Purpose Metrics

- Public-interest outcomes
- research outputs
- standards coherence
- evaluation access
- implementation
- capacity
- affected-party benefit

55.2 Independence Metrics

- Funder concentration
- access concentration
- exclusive relationships
- partner governance rights
- publication disputes
- recusals
- dependence

55.3 Integrity Metrics

- Claim corrections
- logo misuse
- complaints
- incidents
- partner disclosures
- overdue reviews
- contract exceptions

55.4 Participation Metrics

- Regions

- languages
- affected-party participation
- accessibility
- small-organization participation
- compensated public-interest participation

55.5 Security and Data Metrics

- Access reviews
- incidents
- data-return completion
- vendor findings
- protected-information breaches

55.6 Financial Metrics

- Partner funding
- concentration
- in-kind value
- restricted funding
- unpaid commitments
- termination cost

55.7 Exit Metrics

- Time to suspend
- time to correct
- exit readiness
- record recovery
- branding removal
- continuity

55.8 Anti-Metric Rule

Do not treat:

- Partner count
- partner prestige
- logo count
- geographic count
- funding volume
- media reach

as proof of institutional legitimacy.

56. Partnership Audit

56.1 Audit Scope

- Register
- approvals
- due diligence
- conflicts
- funding
- agreements
- data
- intellectual property
- publication
- branding
- security
- human rights
- monitoring
- complaints
- incidents
- renewals
- exits

56.2 Audit Sample

Include:

- Developer
- government
- standards organization
- evaluator
- accreditation body
- academic institution
- civil-society organization
- funder
- infrastructure vendor
- international partner

56.3 Audit Questions

- Is the relationship classified accurately?
- Was approval valid?
- Is the public purpose clear?
- Are risks current?
- Are funding and conflicts visible?
- Are decision rights bounded?

- Are publication rights adequate?
- Is data handled lawfully?
- Is branding accurate?
- Can Standards Body exit?
- Were affected parties engaged?
- Are complaints safe?
- Did corrections propagate?
- Does public status match reality?

56.4 Critical Findings

- Concealed partner control
- false government or international recognition
- publication veto over supported findings
- corruption
- serious retaliation
- unauthorized protected-data use
- false certification or accreditation claim
- undisclosed material funding
- no exit from severe dependency
- partner control of complaint investigation
- material agreement outside approval authority

56.5 Corrective Action

Assign:

- Owner
- deadline
- interim control
- public correction
- relationship status
- verification
- systemic change

56.6 Independent Audit

P4 relationships and high-risk P3 relationships should receive independent review.

57. Partnership Maturity Model

Level 0: Informal Association

Characteristics:

- Meetings
- broad labels
- no register
- no due diligence
- unclear claims

Level 1: Documented Collaboration

Characteristics:

- Purpose
- owner
- written terms
- basic conflict review
- defined output
- exit

Level 2: Governed Partnership System

Characteristics:

- Tiers
- approval
- due diligence
- register
- standard agreements
- funding and branding controls
- annual review

Level 3: Public-Interest Partnership Network

Characteristics:

- Affected-party review
- independent monitoring
- cross-sector balance
- publication independence
- incident and complaint systems
- transparent status

Level 4: Internationally Interoperable Network

Characteristics:

- Regional hubs
- multilingual agreements
- cross-border data controls
- standards liaisons
- recognition mappings
- local capacity

Level 5: Adaptive Institutional Ecosystem

Characteristics:

- Real-time risk monitoring
- diversified dependencies
- auditable public records
- resilient exit
- distributed competence
- independently reviewed authority
- correction across partner systems

57.1 Maturity Rule

A large partner network does not establish mature partnership governance.

58. Consolidated Partnership Failure Modes

58.1 Prestige Partnership

Failure:

A relationship is pursued primarily for the partner's name.

Controls:

- Purpose test
- public-benefit test
- opportunity-cost review

58.2 Logo Laundering

Failure:

A logo implies approval or authority.

Controls:

- Relationship label
- design review
- monitoring
- takedown

58.3 Authority Inflation

Failure:

A government, standards, accreditation, or international relationship is described as recognition beyond its actual status.

Controls:

- Exact classification
- legal review
- public authority note
- correction

58.4 Vendor Inflation

Failure:

An ordinary service provider is called a strategic partner.

Controls:

- Relationship taxonomy
- procurement language
- no prestige labels

58.5 Funder Capture

Failure:

Funding shapes conclusions or priorities improperly.

Controls:

- Restrictions
- concentration limits
- publication independence
- diversification

58.6 Access Capture

Failure:

A model or data provider uses access to influence findings.

Controls:

- Access agreement
- alternatives
- disclosure
- independent methods
- termination

58.7 Standards Capture

Failure:

Beneficiaries of requirements control the standards process.

Controls:

- Balance
- conflict rules
- public review
- consensus
- appeals

58.8 Evaluator Market Capture

Failure:

Evaluator partners design criteria that entrench themselves.

Controls:

- Open criteria
- multiple evaluators
- public-interest review
- accreditation separation

58.9 Government Instrumentalization

Failure:

Standards Body becomes a vehicle for one government's political agenda.

Controls:

- Mission
- public classification
- cross-government pluralism
- independent publication

58.10 Civil-Society Tokenism

Failure:

Organizations are displayed as inclusive participants without meaningful influence.

Controls:

- Defined role
- compensation
- decision record
- feedback disposition

58.11 Community Endorsement Inflation

Failure:

Participation by one organization is treated as endorsement by a whole community.

Controls:

- Representation limits
- public wording
- multiple engagement routes

58.12 Academic Prestige Substitution

Failure:

University affiliation replaces method and operational review.

Controls:

- Research governance
- competence
- quality
- continuity

58.13 Joint-Publication Veto

Failure:

A partner suppresses adverse supported findings.

Controls:

- Publication clause
- separate publication right
- defined embargo
- independent review

58.14 Factual-Review Expansion

Failure:

Partner factual review becomes editorial control.

Controls:

- Defined categories
- comment log
- deadline
- final independent disposition

58.15 Indefinite Embargo

Failure:

Security review prevents publication indefinitely.

Controls:

- Maximum period
- review
- safe summary
- escalation

58.16 Side Agreement

Failure:

An informal promise changes the governed relationship.

Controls:

- Entire-agreement clause
- change approval
- records

58.17 Hidden In-Kind Influence

Failure:

Compute, staff, data, or access is omitted from funding disclosure.

Controls:

- Valuation
- register
- conflict review

58.18 Exclusive Dependence

Failure:

One partner controls an essential capability.

Controls:

- Nonexclusivity
- alternatives
- transition
- board review

58.19 No Exit

Failure:

Termination would destroy the institution's work.

Controls:

- Portability
- archive
- backup
- credentials
- continuity

58.20 Data Appropriation

Failure:

A partner acquires data beyond the approved purpose.

Controls:

- Purpose limitation
- access logs

- audit
- deletion
- sanctions

58.21 Intellectual-Property Lock-In

Failure:

Public-interest work becomes unusable after termination.

Controls:

- Licenses
- background and foreground terms
- archive rights
- open formats

58.22 Confidentiality Overreach

Failure:

Confidentiality conceals misconduct or public-risk information.

Controls:

- Exceptions
- protected disclosure
- independent review
- public minimum

58.23 Security Pretext

Failure:

Security is invoked to suppress criticism.

Controls:

- Specific classification
- security reviewer
- time limits
- redaction

58.24 Partner Claim Drift

Failure:

A partner's public description expands gradually.

Controls:

- Monitoring
- review rights
- correction deadline
- suspension

58.25 Stale Register

Failure:

Ended or suspended relationships remain active publicly.

Controls:

- Status automation
- review dates
- audit

58.26 Complaint Capture

Failure:

Partnership staff control complaints against themselves.

Controls:

- Independent route
- escalation
- governance reporting

58.27 Retaliation

Failure:

A contributor or whistleblower suffers harm for raising a concern.

Controls:

- Nonretaliation
- protected channels
- investigation
- remedy
- termination

58.28 Corruption Through Intermediary

Failure:

A local agent provides improper benefits.

Controls:

- Due diligence
- contract
- payment controls
- audit

58.29 Competition Violation

Failure:

Standards or industry collaboration becomes unlawful coordination.

Controls:

- Counsel
- agendas
- minutes
- information boundaries
- open participation

58.30 Sanctions Evasion

Failure:

A partnership structure circumvents lawful restrictions.

Controls:

- Screening
- legal review
- suspension

58.31 Change-of-Control Neglect

Failure:

A partnership continues after acquisition without review.

Controls:

- Notification
- reassessment
- no automatic transfer

58.32 Partnership Permanence

Failure:

An old relationship continues without present purpose.

Controls:

- End date
- renewal
- outcome review
- completion status

58.33 Partner Count as Legitimacy

Failure:

The institution uses partner volume to imply authority.

Controls:

- Anti-metric rule
- precise claims
- public testing

58.34 Global Representation Theater

Failure:

A geographically diverse logo list is presented as global consensus.

Controls:

- Participation data
- authority limits
- representation disclosure
- development dimension

58.35 Partnership Before Capacity

Failure:

Standards Body accepts a relationship it cannot govern.

Controls:

- Capacity assessment
- staged scope
- decline

- independent support

58.36 Exit Retaliation

Failure:

Parties use legal, financial, access, or reputational pressure to prevent truthful exit.

Controls:

- Agreement
 - records
 - independent governance
 - public correction
 - legal support
-

59. Serious Objections and Responses

Objection 1: Strict partnership controls will make collaboration too slow

Proportional tiers keep low-risk collaboration lightweight.

High-risk relationships should be slower because their effects are larger.

Objection 2: No serious model provider will accept independent publication rights

Some providers may require legitimate security review.

A relationship that permits suppression of supported adverse conclusions should not be described as independent.

Objection 3: Funding always influences priorities

Funding affects capacity and topic selection.

The framework makes that influence visible, diversifies it, and prevents direct control of conclusions and governance.

Objection 4: Government relationships inherently create authority

They create only the authority actually delegated or recognized by law and agreement.

Research, advice, procurement, and regulatory designation remain distinct.

Objection 5: Partner due diligence will become ideological screening

Due diligence should focus on relevant evidence, conduct, risks, authority, conflicts, and the proposed relationship.

It should not require total political agreement.

Objection 6: Human-rights review is outside a technical standards project

Frontier AI standards and evaluations may affect rights, public services, safety, and remedy.

Ignoring those effects would be an institutional design failure.

Objection 7: Civil-society partners are not technically qualified

Technical competence and affected-party knowledge are different contributions.

Neither should replace the other.

Objection 8: Public disclosure will deter partners

Some information may remain protected.

Purpose, funding, roles, authority limits, and current status should ordinarily remain visible.

Objection 9: Joint work requires shared editorial control

Joint statements may require joint approval.

Standards Body should preserve separate publication and correction rights for its own supported conclusions.

Objection 10: Nonexclusivity will prevent valuable privileged access

A limited exclusive arrangement may be justified.

It requires duration, public-interest rationale, alternatives, and enhanced review.

Objection 11: Brand controls are overly defensive

Names and logos create public meaning.

False certification, accreditation, government recognition, or endorsement claims can cause real harm.

Objection 12: Small organizations cannot meet these requirements

Requirements should scale by tier and risk.

Participation support can reduce cost without eliminating core integrity controls.

Objection 13: International work requires broad claims to attract participation

Accurate claims are more durable than premature global branding.

Objection 14: Exit rights make partners less committed

A credible exit protects both parties and prevents dependency from replacing voluntary collaboration.

Objection 15: Standards Body should accept prominent partners early to build legitimacy

Premature prestige relationships can create borrowed legitimacy, capture, and authority inflation.

Credibility should arise from the quality of the work and governance of the relationship.

60. Implementation Pathway

Phase 1: Minimum Partnership Control

- Adopt terminology
- classify existing relationships
- create intake
- create basic due diligence
- define approval authority
- create no-endorsement language
- create partnership register

Phase 2: Agreement Infrastructure

- Create standard agreement modules
- define data and intellectual property
- define publication rights
- define branding
- define complaints
- define exit
- create record system

Phase 3: Material Partnership Governance

- Adopt tier system
- create board review
- create conflict register
- create funding concentration review
- create human-rights review
- create security review
- create annual monitoring

Phase 4: Partner-Type Modules

- Government
- standards
- evaluator and accreditation
- developer
- academic
- civil society
- funder
- international
- vendor

Phase 5: Public Infrastructure

- Publish register
- publish summaries
- add structured metadata
- create corrections
- create public complaint route
- archive ended partnerships

Phase 6: Resilience and Exit

- Map dependencies
- create alternatives
- test data return
- test credential revocation
- test publication after exit
- conduct termination exercise

Phase 7: Audit and International Interoperability

- Conduct independent audit
- test regional agreements
- improve translations

- map standards liaisons
 - publish metrics
 - revise framework
-

61. First Partnership Governance Pilot

61.1 Pilot Title

Material Partnership Review Pilot

61.2 Scope

Apply the framework to three hypothetical or real candidate relationships:

1. Frontier AI model-access provider
2. standards or accreditation institution
3. civil-society or affected-community organization

61.3 Pilot Steps

- Intake
- classification
- tier
- due diligence
- human-rights review
- conflict review
- authority review
- data and intellectual-property terms
- publication terms
- branding terms
- agreement
- public summary
- monitoring plan
- exit drill

61.4 Comparative Questions

- Which risks differ by partner type?
- Which controls are universal?
- Which reviews require external expertise?
- How long does approval take?
- Can public summaries remain useful?
- Are exit rights operational?

- Does the relationship create false authority?
- Can Standards Body publish adverse findings?
- Are affected parties represented?

61.5 Success Criteria

- Relationship type is precise
- public purpose is measurable
- due diligence changes the agreement where needed
- conflicts are visible
- publication independence is preserved
- data and security are governed
- branding cannot imply endorsement
- public summary is accurate
- exit is feasible
- monitoring is assigned

61.6 Pilot Nonclaim

Participation in the pilot does not create approved partner status unless formal approval is granted.

62. Partnership Governance Scorecard

Dimension	Core question
Identity	Are the exact legal parties known?
Classification	Is the relationship type precise?
Tier	Is governance proportionate to materiality?
Purpose	Does the relationship advance a defined public interest?
Necessity	Is partnership the appropriate mechanism?
Authority	Did the correct body approve it?
Nonauthority	Are absent powers and recognition clear?
Mission	Does the relationship fit present identity?
Human rights	Are severe impacts and affected parties addressed?
Independence	Can Standards Body reach and publish its own conclusions?
Capture	Are funding, access, governance, and prestige risks controlled?
Conflicts	Are relevant interests disclosed and managed?
Funding	Are money and in-kind resources transparent and noncontrolling?
Government	Is the legal or contractual relationship described exactly?
Standards	Are liaison, voting, adoption, and consensus rights accurate?

Dimension	Core question
Evaluation	Are developer and evaluator roles separated appropriately?
Data	Are purpose, rights, privacy, provenance, and deletion governed?
Intellectual property	Can work remain usable and correctable?
Publication	Are factual review, embargo, dissent, and correction controlled?
Confidentiality	Are secrets protected without concealing misconduct?
Security	Are access, incidents, and dangerous information governed?
Branding	Can no logo or claim imply unsupported endorsement or authority?
Governance	Are joint and reserved decisions clear?
Competition	Are coordination and exclusion risks controlled?
Corruption	Are improper benefits and intermediaries governed?
Sanctions	Are cross-border restrictions addressed?
Accessibility	Can affected and regional participants engage meaningfully?
Transparency	Is the material relationship publicly registered?
Monitoring	Are outcomes, conflicts, claims, and risks reviewed?
Complaints	Can concerns be raised safely and independently?
Incidents	Can the relationship pause, investigate, and correct?
Renewal	Is continuation a new reasoned decision?
Exit	Can Standards Body leave without losing truth, records, or continuity?
History	Is the complete relationship preserved?
Audit	Can an independent reviewer reconstruct the decision and operation?

62.1 Critical Failures

The following normally prevent approval or require immediate suspension:

- False or concealed legal identity
- unlawful purpose
- bribery or corruption
- unmanageable capture
- predetermined conclusions
- publication veto over supported public-interest findings
- false government, standards, certification, accreditation, or international-recognition claim
- severe unresolved human-rights harm
- unauthorized protected-data use
- no security controls for protected frontier systems
- result-dependent funding
- retaliation
- no credible exit from a severe dependency
- partner control of complaints concerning itself

- exclusive relationship creating unjustified institutional or market control
- agreement approved outside valid authority

62.2 No Composite Score

A critical authority, independence, rights, security, corruption, or publication failure cannot be offset by funding, expertise, or prestige.

63. Partnership Intake Template

Intake ID:

Proposed partner:

Legal entity:

Authorized representative:

Proposer:

Date:

Proposed relationship type:

Proposed tier:

Public-Interest Purpose

Why Partnership Is Necessary

Expected Outcomes

Contributions by Each Party

Funding and In-Kind Resources

Data and System Access

Intellectual Property

Publication

Branding

Duration

Affected Parties

Preliminary Risks

Existing Relationships and Conflicts

Required Review

Intake Decision

- Proceed
- proceed with conditions
- request information
- escalate
- defer
- decline
- prohibit

64. Partnership Due-Diligence Template

Review ID:
Partner:
Relationship:
Tier:
Reviewer:
Date:

Identity and Ownership

Governance

Mission and Conduct

Legal and Regulatory Status

Authority

Financial Condition

Funding and Restrictions

Human-Rights Impacts

Affected Parties and Engagement

Technical Competence

Research or Evaluation Integrity

Security

Privacy and Data

Intellectual Property

Conflicts and Capture

Competition and Antitrust

Anti-Corruption

Sanctions and Export Controls

Public Claims and Branding History

Incidents, Complaints, and Corrections

Dependency and Exit

Partner Response

Residual Risk

Recommendation

- Approve
- approve with conditions
- enhanced monitoring
- limited scope
- defer
- decline
- prohibit

65. Partnership Approval Record Template

Decision ID:

Partner:

Relationship type:

Tier:

Decision authority:

Date:

Purpose

Due-Diligence Findings

Public-Interest Assessment

Conflicts and Recusals

Funding

Authority Implications

Data, Security, and Privacy

Publication and Intellectual Property

Branding and Public Claims

Decision

- Approve
- approve conditionally
- narrow
- defer
- decline
- prohibit

Conditions

Effective Date

Review Date

Term

Termination Authority

Dissent

Public Summary

66. Material Partnership Public Summary Template

Partner:

Legal entity:

Relationship type:

Status:

Start date:

Expected end or review date:

Purpose

Scope

Contributions

Funding and In-Kind Support

Governance

Data and System Access

Intellectual Property

Publication Rights

Branding Rights

Security and Confidentiality

Authority Limits

This relationship concerns the defined purpose and does not imply approval, certification, accreditation, governmental recognition, or endorsement of all activities or positions of either party.

Complaints and Corrections

Current Status and History

67. Conflict and Independence Record Template

Partnership:

Review date:

Owner:

Threat	Source	Severity	Existing control	Residual risk	Decision

Governance Independence

Financial Independence

Methodological Independence

Informational Independence

Operational Independence

Publication Independence

Political Independence

Access Dependence

Client or Funder Concentration

Recusals

Independent Review

Public Disclosure

Reassessment Trigger

68. Model-Access Agreement Schedule Template

Provider:

System:

Model and system version:

Access mode:

Project:

Access period:

Interfaces and Tools

Rate and Use Limits

Safeguards

Logs and Evidence

System Changes

Task Independence

Provider Personnel

Confidentiality

Security

Factual Review

Publication Review Period

Embargo

Adverse Findings

Corrections

Access Withdrawal

Unrelated Access Nonretaliation

Marketing and Public Claims

Post-Access Records

69. Joint Research Agreement Schedule Template

Project:

Parties:

Research owner:

Protocol ID:

Registration:

Research Question

Methods

Data

Systems

Human Participants

Roles

Authorship and Contributions

Funding

Analysis Independence

Partner Review

Publication

Dissent and Separate Publication

Intellectual Property

Security and Confidentiality

Corrections and Retractions

Archive

Exit

70. Standards Liaison Record Template

Relationship ID:

Organization:

Committee or program:

Liaison type:

Start date:

Review date:

Procedural Basis

Participation Rights

- Attend
- submit
- nominate
- comment
- observe
- vote
- access documents

Representative

Conflicts

Information Exchange

Confidentiality

Public Reporting

Standards Status Limits

Renewal or Termination

71. Government Relationship Record Template

Government entity:

Jurisdiction:

Relationship type:

Legal or contractual basis:

Start date:

Status:

Purpose

Authority Granted

Authority Not Granted

Funding

Deliverables

Publication Rights

Public-Record Obligations

Confidentiality and Security

Human-Rights Review

Political-Activity Limits

Audit and Oversight

Public Description

Review and Exit

72. Data-Sharing Schedule Template

Data set or system:

Provider:

Recipient:

Purpose:

Term:

Data Description

Provenance

Ownership

Legal Roles

Lawful Basis

Permitted Uses

Prohibited Uses

Access

Security

Personal Data

Cross-Border Transfer

Derived Data

Audit

Incident Notice

Correction

Retention

Return or Deletion

Post-Termination

73. Intellectual-Property Schedule Template

Partnership:

Effective date:

Background Intellectual Property

Foreground Intellectual Property

Joint Work

Code

Data

Methods

Standards Contributions

Patents

Copyright

Trademarks

Licenses

Attribution

Publication

Maintenance

Security Restrictions

Post-Termination Rights

Archive Rights

74. Publication Review Log Template

Output:

Version:

Partner:

Review period:

Comment	Category	Evidence	Disposition	Decision owner
	Factual			
	Confidentiality			
	Security			
	Legal			
	Editorial			

Embargo

Unresolved Disagreement

Partner Response

Independent Conclusion

Publication Decision

Correction Route

75. Branding Authorization Template

Partner:

Authorized asset:

Purpose:

Channels:

Start:

End:

Approved Relationship Language

Required Scope and Status

No-Endorsement Language

Prohibited Uses

Placement Rules

Review Rights

Monitoring

Correction Deadline

Suspension

Post-Exit Removal

76. Partnership Monitoring Record Template

Partnership:

Review period:

Reviewer:

Tier:

Purpose and Outcomes

Deliverables

Funding

Conflicts

Independence

Human Rights

Affected-Party Feedback

Data and Privacy

Security

Publication

Branding and Public Claims

Complaints

Incidents

Dependency

Legal and Organizational Changes

Renewal Recommendation

- Continue
- continue with conditions
- narrow
- suspend
- complete
- terminate

77. Partnership Incident Record Template

Incident ID:
Partnership:
Detected:
Severity:
Owner:

Incident Type

Affected People, Systems, Data, or Publications

Immediate Risk

Containment

Evidence Preservation

Partner Notification

External Notification

Investigation

Root Cause

Public-Reliance Effect

Correction

Partnership Status

Remediation

Continuation Decision

Public Notice

Closure

78. Suspension and Termination Record Template

Partnership:

Action: Suspension or termination

Authority:
Effective date:

Grounds

Immediate Effect

Active Work

Funding

Data and Access

Intellectual Property

Publication

Branding

Confidentiality

People and Affected Parties

Records and Archive

Public Statement

Corrections

Disputes

Post-Exit Monitoring

79. Partnership Dependency Register Template

Dependency	Partner	Criticality	Alternatives	Switching time	Exit effect	Mitigation	Owner

Concentration Findings

Single Points of Failure

Required Diversification

Continuity Test

Review Date

80. Partnership Audit Template

Audit period:

Auditor:

Independence:

Scope:

Register Completeness

Classification and Tiering

Approval Authority

Due Diligence

Mission and Public Interest

Human Rights

Conflicts and Capture

Funding and In-Kind Resources

Government and Standards Claims

Developer and Evaluator Relationships

Data and Privacy

Intellectual Property

Publication Independence

Security and Confidentiality

Branding and Public Claims

Competition and Anti-Corruption

Complaints and Whistleblowing

Incidents and Corrections

Monitoring and Renewal

Suspension, Termination, and Exit

Critical Findings

Material Findings

Corrective Actions

Public Summary

81. Canonical Standards Body Partnership Positions

Standards Body adopts the following working positions.

1. Partnership is a governed relationship, not a prestige label.
2. Every material partnership should advance a defined public-interest purpose.
3. Mission outranks funding, access, visibility, and partner prestige.
4. A partnership should be used only when it produces value that unilateral work cannot provide as well.
5. Relationship types should be described precisely.
6. Vendor, contractor, funder, sponsor, liaison, collaborator, and partner should remain distinct.
7. Strategic partner is an authority-sensitive term requiring enhanced approval.
8. A relationship does not create endorsement.
9. A relationship does not create membership.
10. A relationship does not create certification.
11. A relationship does not create accreditation.
12. A relationship does not create governmental authority.
13. A relationship does not create international recognition.
14. Standards Body does not currently exercise public regulatory, certification, or accreditation authority.
15. Partner claims should preserve Standards Body's present institutional stage.
16. Every material relationship should identify authority that exists and authority that does not.
17. Private agreements should not create hidden public-governance authority.
18. A board-approved relationship does not imply approval of the partner generally.
19. Approval should scale with materiality.
20. Authority-shaping and entity-forming partnerships require constitutional review.
21. Partnership tier is a risk category, not a status reward.
22. A public announcement should not precede approval.
23. Due diligence should be proportionate to consequence and dependence.
24. Prestigious institutions should not receive reduced due diligence.
25. Government, nonprofit, academic, industry, and civil-society categories do not establish trust automatically.

26. Due diligence should examine actual ownership, conduct, authority, conflicts, security, rights, and exit.
27. Proposed partners should have an opportunity to respond to material adverse information.
28. Standards Body should decline relationships it lacks capacity to govern.
29. Public benefit should be identified beyond institutional growth.
30. Opportunity cost should be considered.
31. Human-rights due diligence should examine causation, contribution, and direct linkage.
32. Severe human-rights risk should receive priority.
33. Affected-party engagement should be capable of changing the decision.
34. Participation should be safe, accessible, timely, and nonretaliatory.
35. A technically useful partnership should not ignore severe public-interest harm.
36. Human-rights defenders, whistleblowers, workers, and researchers should be protected.
37. A grievance mechanism does not replace broader affected-party engagement.
38. Partnership should preserve access to remedy.
39. Independent judgment is a nonnegotiable institutional asset.
40. Independence should be assessed across governance, funding, methods, information, operations, publication, personnel, security, and politics.
41. Funding dependence and access dependence should be recorded.
42. Standards Body should diversify critical dependencies.
43. No partner should receive a permanent veto over institutional conclusions or corrections.
44. No partner should receive a governing seat solely because of funding or access.
45. Access providers should not threaten unrelated access to influence findings.
46. Material partnerships should receive capture review.
47. Institutional conflicts may exist even without individual conflicts.
48. A party benefiting from a standard should not control the standard.
49. A developer should not control an independent evaluation of its own system.
50. A funder should not control findings.
51. Advocacy commitments should be disclosed without automatic exclusion.
52. Unmanageable conflicts require refusal or termination.
53. Funding should support work, not purchase conclusions.
54. Result-dependent funding is prohibited.
55. Standards outcomes, accreditation decisions, certification decisions, and evaluation results should not be contingent-payment events.
56. In-kind resources should be valued and disclosed.
57. Model access, compute, staff, data, and facilities can create influence comparable to money.
58. Restricted funding should not create hidden ownership of the research agenda.
59. Material funding should be published under the transparency framework.
60. Government relationships should identify their exact legal or contractual form.
61. Research, advice, procurement, recognition, delegation, regulation, and enforcement should remain distinct.
62. Government collaboration should not be described as public authority without a valid basis.
63. Standards Body should remain capable of criticizing a government partner lawfully.
64. Political neutrality does not require silence concerning evidence or rights.
65. A delegated function requires legal basis, governance, competence, appeal, public notice, and identity change.

66. Standards liaisons should be described according to actual procedural rights.
67. Participation in a standards committee does not imply voting rights or adoption.
68. Joint work does not become an international standard merely because the parties operate internationally.
69. Standards partnerships should support transparency, openness, impartiality, consensus, relevance, coherence, and development.
70. Standards cooperation should reduce duplication.
71. Proprietary references should not become hidden barriers without justification.
72. Joint standards work should define process, copyright, maintenance, appeals, and status.
73. Competition law applies to standards and industry partnerships.
74. Evaluator partners should not design criteria solely to entrench their own market position.
75. Pilot qualification should not be described as accreditation.
76. Relationships with accreditation bodies should not make Standards Body an accreditation body.
77. Relationships with certification bodies should define the scheme and decision authority.
78. Assurance relationships should preserve role separation.
79. Frontier developer partnerships require enhanced review.
80. The exact model, system, version, access mode, and restrictions should be recorded.
81. Provider factual review should not become editorial veto.
82. Factual, confidentiality, security, legal, and methodological review comments should remain distinguishable.
83. Partner review periods should be time bounded.
84. Legitimate security embargoes should have defined release conditions.
85. Indefinite suppression of adverse findings is incompatible with independent public-interest research.
86. Developers should not use partnership status to claim approval, safety, certification, or endorsement.
87. Funding and access from the same developer should be disclosed together.
88. Comparative evaluation should use sufficiently comparable access conditions.
89. Task design and custody should remain independent where independent evaluation is claimed.
90. Academic prestige does not replace method, ethics, quality, or continuity.
91. Students and trainees should receive supervision, credit, protection, and nonretaliation.
92. Academic freedom should be preserved within lawful security and confidentiality limits.
93. University names should not imply institutional endorsement without authorization.
94. Civil-society participation should not be symbolic.
95. A civil-society partner should be compensated for meaningful work where appropriate.
96. One organization should not be presented as representing an entire community without mandate.
97. Participation does not imply community endorsement.
98. Civil-society partners should remain free to criticize Standards Body.
99. International partner diversity does not equal global consensus.
100. Regional partnerships should include local law, language, institutions, infrastructure, and affected-party knowledge.
101. International work should not extract expertise or data without durable local benefit.

102. Cross-border data sharing should address transfer, security, access, retention, and remedy.
103. Formal mutual recognition should not be claimed without an actual arrangement.
104. Donor influence should be visible.
105. Anonymous funding requires enhanced internal review.
106. Naming rights should not create permanent influence.
107. Funders should not receive technical decision rights merely because they financed the work.
108. Open-source communities can provide methods, review, and global participation.
109. Formal institutional obligations still require accountable maintainers or legal structures where necessary.
110. Open methods can coexist with protected tasks.
111. Repository participation does not imply endorsement by all contributors.
112. Ordinary vendors should be described as vendors.
113. Critical vendors require security, continuity, portability, and exit controls.
114. Protected information should not be submitted to unauthorized AI services.
115. Joint research should identify who controls question, method, analysis, publication, and correction.
116. A partner may contribute data without owning the conclusion.
117. A partner may disagree without erasing the institutional record.
118. Joint outputs should identify which parties approved which conclusions.
119. A bilateral technical document should not be presented as broad consensus.
120. Every joint work product should have an owner, version, source register, correction route, review date, and archive.
121. Data use should be lawful, necessary, purpose limited, and traceable.
122. Derived data rights should be defined.
123. Data should be returned, deleted, or retained according to law and agreement after exit.
124. Background and foreground intellectual property should remain distinct.
125. Public-interest work should remain inspectable and usable where lawful.
126. Standards should not depend unnecessarily on inaccessible proprietary rights.
127. Patent interests relevant to standards work should be disclosed under the applicable process.
128. Publication rights should be negotiated before work begins.
129. Partner review should protect facts, confidentiality, security, and law, not suppress supported criticism.
130. A partner should be able to publish a response.
131. Standards Body should retain correction authority over its own work.
132. Termination should not automatically suppress completed lawful research.
133. Confidentiality should protect legitimate secrets without becoming a shield for misconduct.
134. Protected-disclosure and legal-reporting exceptions should be preserved.
135. Security classification should be specific and reviewable.
136. Security should not be used as a pretext for reputation management.
137. Brand use should describe the relationship rather than manufacture authority.
138. Standards Body should not issue partnership badges resembling certification or accreditation marks.
139. Every logo use should include a relationship context where misunderstanding is plausible.
140. Post-exit brand use should be limited to accurate historical reference.

141. Joint communications should distinguish shared statements from attributed positions.
142. Partners may disagree publicly.
143. A steering committee should not control Standards Body's identity or independent conclusions.
144. Joint and reserved decisions should be defined.
145. Deadlock procedures should permit separate publication, scope reduction, or exit.
146. No joint process should prevent correction of a false statement.
147. Partnership agreements should address purpose, contributions, governance, independence, funding, data, intellectual property, publication, confidentiality, security, branding, monitoring, complaints, and exit.
148. Side agreements should not alter material public-interest controls without approval.
149. Payment should be for work, not favorable outcome.
150. Related-party transactions should be disclosed.
151. Partnerships should not facilitate price coordination, market allocation, boycotts, procurement manipulation, or exclusion.
152. Standards meetings should control exchange of commercially sensitive information.
153. Technical requirements should be justified by evidence rather than competitor exclusion.
154. Bribery and improper benefits are prohibited.
155. Intermediaries should receive due diligence.
156. Gifts, hospitality, future jobs, data access, and research funding may create improper influence.
157. Accurate books and records are required.
158. Serious corruption may require immediate termination.
159. Applicable sanctions and export controls should be reviewed.
160. A partnership should not be structured to evade law.
161. Standards Body may participate in policy processes without becoming a partisan campaign organization.
162. Joint lobbying should be disclosed where material.
163. A public official's participation does not imply government endorsement.
164. Environmental costs of compute, infrastructure, and travel should be considered.
165. Sustainability claims should be evidenced.
166. Accessibility should apply to meetings, documents, tools, comments, and outputs.
167. Language, time zone, bandwidth, and participation cost shape real inclusion.
168. A partnership claiming inclusion should provide practical participation access.
169. Material partnerships should appear in a public register.
170. Public summaries should identify purpose, funding, governance, data, intellectual property, publication, branding, and authority limits.
171. Protected details may remain confidential while a public minimum remains visible.
172. Ended partnerships should remain historically discoverable.
173. Monitoring should examine outcomes and risks, not only deliverables.
174. Partner self-reporting should not be the only monitoring source.
175. Renewal is a new decision.
176. Material ownership, funding, leadership, legal, security, and public-claim changes should trigger review.
177. Complaints should be available to affected parties and insiders.

178. A person implicated in a complaint should not control the investigation.
 179. Good-faith reporting should be protected from retaliation.
 180. Nondisparagement and confidentiality clauses should not prohibit lawful protected disclosure.
 181. Material incidents should affect partnership status visibly.
 182. An implicated partner should not control the complete incident investigation.
 183. Public corrections should travel to every channel carrying the original claim.
 184. Refusal to correct a materially false partnership claim may justify suspension or termination.
 185. Suspension may be partial.
 186. Critical risk may require immediate suspension.
 187. Exit rights should protect evidence, people, data, publications, corrections, and continuity.
 188. Partnerships should not become hostage relationships.
 189. A change of control should trigger review.
 190. Partnerships should not transfer automatically to a materially different legal entity.
 191. Partner failure plans should preserve records and public status.
 192. Partner count and funding volume are not legitimacy metrics.
 193. Prestige does not offset a critical rights, authority, security, corruption, or independence failure.
 194. Material partnerships should be auditable.
 195. P4 and high-risk P3 relationships should receive independent review.
 196. The present goal is a governed network, not a collection of logos.
 197. Standards Body should prefer several bounded relationships over one dominant dependency.
 198. It should remain possible to collaborate, disagree, correct, and leave.
 199. Partnership history should not be erased after termination.
 200. The ultimate partnership test is whether the relationship produces public value while leaving Standards Body able to tell the truth, govern itself, protect people, and exit without surrendering its institutional record.
-

82. Relationship to Other Canonical Files

PROJECT_IDENTITY.md

Controls Standards Body's mission, present stage, authority, nonauthority, and approved public descriptions.

No partnership may alter identity through implication.

PROJECT_MANIFESTO.md

Provides the long-term public-interest purpose against which partnership opportunities should be assessed.

INSTITUTION_DESIGN.md

Defines the distributed institutional ecosystem and the functions that should remain separated across partners.

GOVERNANCE_FRAMEWORK.md

Defines approval authority, reserved matters, conflicts, funding, major partnerships, government relationships, international governance, complaints, appeals, and institutional transitions.

STANDARDS_DEVELOPMENT_PROCESS.md

Governs standards liaisons, joint technical work, balance, consensus, public review, intellectual property, normative references, maintenance, and withdrawal.

EVALUATOR_ACCREDITATION_FRAMEWORK.md

Governs partnerships with evaluators, certification bodies, accreditation bodies, proficiency-testing providers, and assurance institutions.

TRANSPARENCY_FRAMEWORK.md

Defines public partnership summaries, funding disclosures, protected information, public minimums, incidents, corrections, and records.

CONTRIBUTOR_FRAMEWORK.md

Defines individual and institutional representative roles, conduct, access, credit, confidentiality, intellectual property, security, conflicts, and exit.

WEBSITE_SOURCE_OF_TRUTH.md

Defines public partnership pages, logo use, authority claims, status, structured data, corrections, and archives.

SOURCES.md

Defines due-diligence sources, source currentness, conflicting evidence, protected sources, and corrections.

VERSION_HISTORY.md

Defines partnership versions, status changes, agreement amendments, corrections, suspension, termination, and historical preservation.

TERMINOLOGY.md

Controls partnership, liaison, sponsor, funder, evaluator, accreditation, certification, recognition, and authority language.

TAXONOMY.md

Classifies partners, relationship types, contributions, risks, decisions, status, and institutional roles.

EVIDENCE_STANDARDS.md

Defines the evidence required for due diligence, public claims, research findings, conflict assessment, and partnership decisions.

RESEARCH_METHODOLOGY.md

Governs joint research design, sources, registration, ethics, analysis, review, publication, correction, and AI-tool use.

EVALUATION_PHILOSOPHY.md

Governs model-access and evaluator relationships, result interpretation, validity, uncertainty, and evaluation limits.

Foundation 1

Requires partnership control over protocol ownership, versioning, dynamic updates, comparability, and bridge studies.

Foundation 2

Requires controlled relationships for held-out tasks, secure access, custody, compromise, and protected evidence.

Foundation 3

Requires enhanced review for partnerships involving high-stakes capability evaluation and dangerous information.

Foundation 4

Requires independent expert review, conflict controls, publication rights, dissent, and appeals.

Foundation 5

Requires clear separation among evaluator, audit, certification, accreditation, scheme, and recognition functions.

Foundation 6

Requires partnership distinctions among research, guidance, standards, procurement, legal recognition, mandate, and enforcement.

Foundation 7

Requires funding, prestige, awards, rankings, and recognition relationships to resist gaming and capture.

Foundation 8

Requires international partnerships to preserve semantic, legal, technical, linguistic, and institutional interoperability without claiming universal authority.

83. Final Partnership Position

Standards Body will require partners.

It should not require borrowed authority.

The institution should be able to work with:

- Governments without becoming a government
- standards organizations without claiming standards status it does not possess
- developers without becoming their evaluator of convenience
- evaluators without controlling their accreditation
- accreditation bodies without claiming accreditation authority
- funders without selling conclusions
- civil society without claiming complete community representation
- universities without substituting prestige for evidence
- international institutions without claiming global consensus
- vendors without calling procurement a strategic alliance

The partnership system should make several questions easy to answer:

- Why does the relationship exist?
- What does each party contribute?
- Who pays?
- Who decides?
- Who owns the work?

- Who controls data?
- Who controls publication?
- What information is protected?
- What authority exists?
- What authority does not exist?
- Which conflicts remain?
- Who may complain?
- What happens after an incident?
- Can the relationship be corrected?
- Can Standards Body leave?
- What remains after exit?

A strong partner should not need Standards Body to exaggerate the relationship.

A strong Standards Body should not need a partner's logo to substitute for institutional competence.

The measure of a partnership is not closeness.

It is whether collaboration improves the work without degrading:

- Truth
- evidence
- independence
- rights
- security
- accessibility
- due process
- public accountability
- institutional continuity

The defining partnership principle is:

Accept expertise, access, funding, implementation, and cooperation only under terms that preserve bounded authority, independent judgment, public-interest responsibility, truthful communication, and a credible right to exit.

References and Research Basis

[^ungp]: United Nations Office of the High Commissioner for Human Rights, **Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework**. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[^hrd-guidance]: United Nations Working Group on Business and Human Rights, **The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights**

Defenders. https://www.ohchr.org/sites/default/files/2022-02/Formatted-version-of-the-guidance-EN_0.pdf

[^oecd-due]: Organisation for Economic Co-operation and Development, **OECD Due Diligence Guidance for Responsible Business Conduct.** <https://mneguidelines.oecd.org/due-diligence-guidance-for-responsible-business-conduct.htm>

[^oecd-ai]: Organisation for Economic Co-operation and Development, **OECD AI Principles,** updated in May 2024. <https://oecd.ai/en/ai-principles>

[^unesco-ai]: United Nations Educational, Scientific and Cultural Organization, **Recommendation on the Ethics of Artificial Intelligence.** <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>

[^coe-ai]: Council of Europe, **Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law,** CETS No. 225. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>

[^wto-tbt]: World Trade Organization, **Agreement on Technical Barriers to Trade,** including Annex 3, Code of Good Practice for the Preparation, Adoption and Application of Standards. https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm

[^wto-six]: World Trade Organization, Technical Barriers to Trade Committee, **Principles for the Development of International Standards, Guides and Recommendations.** https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm

[^iso-directives]: International Organization for Standardization and International Electrotechnical Commission, **ISO/IEC Directives, Part 1, Procedures for the Technical Work,** Consolidated ISO Supplement. <https://www.iso.org/sites/directives/current/consolidated/index.html>

[^nist-ai-rmf]: National Institute of Standards and Technology, **Artificial Intelligence Risk Management Framework 1.0** and associated resources. <https://www.nist.gov/itl/ai-risk-management-framework>

[^uncac]: United Nations, **United Nations Convention against Corruption.** <https://www.unodc.org/unodc/en/treaties/CAC/>

[^crpd]: United Nations, **Convention on the Rights of Persons with Disabilities.** <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities>

[^iso26000]: International Organization for Standardization, **ISO 26000:2010, Guidance on social responsibility.** <https://www.iso.org/standard/42546.html>

[^iso37001]: International Organization for Standardization, **ISO 37001:2025, Anti-bribery management systems, Requirements with guidance for use.** <https://www.iso.org/standard/37001>

[^iso37301]: International Organization for Standardization, **ISO 37301:2021, Compliance management systems, Requirements with guidance for use.** <https://www.iso.org/standard/75080.html>

[^iso31000]: International Organization for Standardization, **ISO 31000:2018, Risk management, Guidelines**. <https://www.iso.org/standard/65694.html>

[^iso27001]: International Organization for Standardization and International Electrotechnical Commission, **ISO/IEC 27001:2022, Information security management systems, Requirements**. <https://www.iso.org/standard/27001>

[^w3c-wcag]: World Wide Web Consortium, **Web Content Accessibility Guidelines 2.2**. <https://www.w3.org/TR/WCAG22/>

Revision Record

Version 1.0

Date: July 16, 2026

Change type: Complete foundational edition

Summary: Establishes the canonical Standards Body partnership-governance framework. Defines present authority limits, partnership architecture, partner categories, relationship types, tiers, approval authority, intake, due diligence, mission and public-interest fit, human-rights review, independence, capture, conflicts, funding, government relationships, standards liaisons, evaluator and accreditation relationships, developer and model-provider relationships, academic partnerships, civil-society and affected-community participation, international and regional cooperation, philanthropic funding, open-source communities, vendors, joint research, standards work, evaluation access, data governance, intellectual property, publication rights, confidentiality, security, branding, public communications, decision rights, agreement architecture, procurement, competition, anti-corruption, sanctions, political activity, environmental considerations, accessibility, transparency, monitoring, complaints, whistleblowing, incidents, corrections, renewal, suspension, termination, continuity, metrics, audits, maturity, failure modes, objections, implementation, pilot design, scorecard, operational templates, canonical positions, cross-file relationships, primary references, and complete revision record.

Status: Approved foundational source.