

AIP code of conduct

The Agent Interoperability Protocol project is committed to a professional, inclusive, and safe technical community. Everyone who participates in a project space must respect other people and the users affected by protocol, security, connec

SECTION	Project and Releases
TYPE	Project policy
PROTOCOL	AIP 1.0
SOURCE	CODE_OF_CONDUCT.md

This policy applies to contributors, maintainers, reviewers, operators, speakers, representatives, and guests. Participation is conditioned on following it.

Expected behavior

Participants are expected to:

- discuss technical claims with specific reasoning while respecting uncertainty and different experience levels;
- critique code, designs, evidence, and decisions without attacking the person who proposed them;
- communicate directly, patiently, and constructively;
- make room for people with different backgrounds, identities, abilities, locations, and levels of familiarity with the project;
- respect consent, personal boundaries, privacy, and confidential information;
- disclose relevant technical limitations, conflicts of interest, and security impact;
- accept correction and update claims when stronger evidence becomes available;
- follow a maintainer's bounded moderation or incident-safety direction;
- take responsibility for harm and participate in reasonable repair when possible.

Unacceptable behavior

The following behavior is not acceptable:

- harassment, threats, intimidation, stalking, or incitement of violence;
- discriminatory language or conduct based on identity or protected characteristics;

- personal insults, demeaning comments, sexualized content, or unwelcome sexual

or personal attention;

- deliberate misgendering, outing, or publication of private information

without explicit permission;

- sustained disruption of reviews, issues, releases, events, or community

communication;

- coercion, impersonation, or misuse of project authority;

- knowingly false technical, security, conformance, or qualification claims;

disclosure of credentials, customer data, embargoed vulnerabilities, private report details, or protected deployment information;

- retaliation against a person who reports or helps review a concern in good

faith;

- deliberately false, fabricated, or retaliatory reports.

A good-faith report is not a violation merely because it is incomplete, mistaken, or cannot be substantiated.

Keep technical disagreement rigorous and respectful

Firm technical review is part of the project. Maintainers and reviewers may reject a change, request evidence, limit a risky operation, or correct an unsupported claim. A decision that someone disagrees with is not by itself a conduct violation.

Technical authority does not permit harassment, humiliation, retaliation, or selective enforcement. Apply the same evidence and behavior standard to maintainers, established contributors, and newcomers.

Scope

This policy applies in:

- repositories, reviews, issues, and project-managed automation;
- project-operated chat, email, meetings, events, and support channels;
- release, conformance, qualification, incident, and disclosure activities;
- public situations where a participant is formally representing the project;
- private communication that directly affects safety or participation in a

project space.

Project maintainers can moderate project-controlled spaces and can ask a repository host or relevant organization to act within its authority. This policy does not give maintainers authority over unrelated private life, external communities, emergency response, employment disputes, or legal proceedings.

Report a conduct concern

Send conduct reports privately to with the subject prefix `[CONDUCT]`. Do not place personal, safety, credential, customer, or private report information in a public issue or review.

If there is immediate danger, contact the appropriate local emergency service or the platform's urgent-safety channel. The AIP project is not an emergency service.

Report a software vulnerability through the separate process in [SECURITY.md](#). Use `[CONDUCT]` when the concern is about behavior, including behavior that occurred during vulnerability handling.

Include what is available and safe to share:

- the project space, approximate date and time, and people involved;
- what happened and how it affected participation or safety;
- relevant links, messages, screenshots, or witnesses;
- any immediate safety or privacy concern;
- a requested communication method or protective measure, if any;
- whether a maintainer or reviewer has a conflict of interest.

You do not need to investigate, confront the reported person, collect every record, or prove the concern before reporting it. Preserve original records when safe, and avoid gathering unrelated personal information.

How reports are handled

The project will use this process:

1. A maintainer acknowledges the report when practical and identifies the next communication step. The project does not publish a fixed response-time SLA.
2. Anyone named in the report or unable to act impartially must recuse from the decision.
3. The reviewer limits access to people needed to assess safety, facts, conflicts, and possible action.
4. The reviewer may ask the reporter, reported person, or witnesses for relevant context without requiring unsafe contact between them.
5. Temporary restrictions may be used while reviewing an immediate safety, privacy, retaliation, or disruption risk. A temporary measure is not a final finding.
6. The reviewer evaluates severity, impact, frequency, context, prior relevant behavior, cooperation, and risk of recurrence.
7. When action is taken, affected participants receive the decision and the information they need to follow it, subject to privacy and safety limits.

The project cannot promise anonymity or absolute confidentiality. Report information will be limited to a need-to-know basis, but disclosure may be required for safety, legal obligations, repository-host action, or a fair review. When permitted and safe, the reviewer will tell the reporter before a material disclosure.

Records must contain only information needed for review, enforcement, follow-up, or required obligations. They must not be reused for unrelated purposes.

Enforcement

Maintainers may apply one or more proportionate actions:

1. a clarification, correction, or request to stop;
2. removal or editing of harmful content;

3. a private or formal warning with stated expectations;
4. a temporary restriction from a discussion, review, role, event, or project space;
5. removal of project permissions or representative status;
6. permanent removal from project-controlled spaces;
7. escalation to the repository host, service provider, relevant organization, or appropriate authority when necessary.

An enforcement notice should identify the policy boundary, required action, effective scope, duration when temporary, and available appeal path. It need not disclose another person's private information or the complete report.

Maintainers may reject or remove contributions independently of conduct enforcement when they are unsafe, out of scope, technically unsupported, or not ready. Do not describe an ordinary technical rejection as disciplinary action unless this policy is actually invoked.

Appeal a conduct decision

Send an appeal to with the subject prefix `[CONDUCT APPEAL]`. Identify the decision and explain a material factual error, process conflict, disproportionate action, or relevant new information. Disagreement alone does not require a different outcome.

An uninvolved maintainer should review the appeal when one is available. If no unconflicted maintainer is available, the project may ask the relevant organization or repository host to review the part within its authority. The project does not guarantee an external reviewer or a particular appeal outcome.

Protective measures remain in effect during an appeal unless the reviewer changes them.

Maintainer responsibility

Maintainers are subject to this policy. They are responsible for applying it consistently, documenting decisions proportionately, protecting report data, addressing retaliation, disclosing conflicts, and correcting enforcement when an appeal identifies a material error.

Using private report information for unrelated technical, commercial, or personal purposes is itself unacceptable behavior.

Related documentation

- [Contributing to AIP](#)
- [Security policy](#)
- [Licensing and usage terms](#)