

Question ID	Question Title	Available options	OpenAI	xAI	Z.ai	Anthropic	Google Deepmind
Q1	Does your company have a WB policy & function covering frontier AI-focused staff? Is this policy publicly accessible without login credentials?	• Prefer not to answer (skips whistleblowing section) • No WB policy & function - (skips whistleblowing section) • Non-public policy exists - Please briefly explain your rationale for keeping it private:	Public WB policy - Please provide URL here: OpenAI's Raising Concerns Policy Blog Copy of Raising Concerns Policy (10.2024)	Non-public policy exists - Please briefly explain your rationale for keeping it private:	Prefer not to answer (skips whistleblowing section)	Non-public policy exists - Please briefly explain your rationale for keeping it private: Please see “post deployment monitoring” in our transparency hub. We expect to share more publicly in the near future. Anthropic's Transparency Hub: Voluntary Commitments	Public WB policy - Please provide URL here: Our code of conduct is public and we have several internal policies that cover whistleblowing. Google Code of Conduct
Q2	Who is formally designated with primary responsibility for overseeing the whistleblowing function and ensuring reports are properly addressed?	• Board/Audit Committee • Executive management • Compliance/Legal department • HR department • Other (Please also specify whom this role reports to):	• Board/Audit Committee • Compliance/Legal department • HR department	• Compliance/ Legal department			• Board/Audit committee • Compliance/Legal and • HR department
Q3	Which statement best describes the investigative independence of your whistleblowing function?	• The whistleblowing function requires approval from management before initiating investigations based on whistleblower reports. • The whistleblowing function can independently initiate and conduct investigations based on whistleblower reports, including those involving senior management. • The whistleblowing function can independently initiate and conduct investigations based on whistleblower reports, including those involving senior management, AND has the authority to engage external expertise without approval.	The whistleblowing function can independently initiate and conduct investigations based on whistleblower reports, including those involving senior management, AND has the authority to engage external expertise without approval.	The whistleblowing function can independently initiate and conduct investigations based on whistleblower reports, including those involving senior management, AND has the authority to engage external expertise without approval.		The whistleblowing function can independently initiate and conduct investigations based on whistleblower reports, including those involving senior management, AND has the authority to engage external expertise without approval.	The whistleblowing function can independently initiate and conduct investigations based on whistleblower reports, including those involving senior management, AND has the authority to engage external expertise without approval.
Q4	Which of the following concerns are explicitly covered by your whistleblowing policy? (Select all that apply)	• Violations of applicable laws and regulations • Violations of the company's public AI safety framework (e.g., Anthropic's Responsible Scaling Policy) • Credible safety concerns that may not violate specific policies including loss-of-control scenarios • Pressure to compromise safety standards or suppress safety concerns • Misleading communications about AI capabilities to external parties (such as regulators, the public, or evaluators) or discrepancies between public claims and internal practices • None of the above	• Violations of applicable laws and regulations • Violations of the company's public AI safety framework (e.g., Anthropic's Responsible Scaling Policy) • Credible safety concerns that may not violate specific policies including loss-of-control scenarios • Pressure to compromise safety standards or suppress safety concerns	• Violations of applicable laws and regulations		• Violations of applicable laws and regulations • Violations of the company's public AI safety framework (e.g., Anthropic's Responsible Scaling Policy) • Credible safety concerns that may not violate specific policies including loss-of-control scenarios • Pressure to compromise safety standards or suppress safety concerns • Misleading communications about AI capabilities to external parties (such as regulators, the public, or evaluators) or discrepancies between public claims and internal practices	• Violations of applicable laws and regulations • Violations of the company's public AI safety framework (e.g., Anthropic's Responsible Scaling Policy) • Credible safety concerns that may not violate specific policies including loss-of-control scenarios • Pressure to compromise safety standards or suppress safety concerns • Misleading communications about AI capabilities to external parties (such as regulators, the public, or evaluators) or discrepancies between public claims and internal practices
Q5	Does your whistleblowing policy explicitly protect individuals who report concerns in 'good faith' or with 'reasonable cause to believe', rather than requiring certainty that violations occurred?	• Yes • No	Yes	Yes		Yes	Yes
Q6	Which of the following persons are protected from retaliation under your whistleblowing policy? (Select all that apply)	• Current employees • Former employees • Contractors and self-employed workers • AI research collaborators and academic partners • Individuals who assist whistleblowers • Suppliers and vendors with access to company systems	• Current employees • Contractors and self-employed workers			• Current employees • Former employees • Contractors and self-employed workers • AI research collaborators and academic partners • Individuals who assist whistleblowers • Suppliers and vendors with access to company systems	• Current employees • Former employees • Contractors and self-employed workers • AI research collaborators and academic partners • Individuals who assist whistleblowers • Suppliers and vendors with access to company systems
Q7	To which of the following individuals or entities can whistleblowers submit reports according to your policy? (Select all that apply)	• Board member or board committee • Dedicated Ethics/Whistleblowing Officer • Ombudsperson • Chief Compliance or Risk Officer • General Counsel/Legal Department • Human Resources department • External/independent third party • Direct disclosure to a statutory or supervisory authority • Other (please briefly specify):	• Board member or board committee • Chief Compliance or Risk Officer • General Counsel/Legal Department • Human Resources department • External/independent third party • Direct disclosure to a statutory or supervisory authority	• General Counsel/Legal Department • Human Resources department • Direct disclosure to a statutory or supervisory authority • Other (please briefly specify): • Manager			• Board member or board committee • Dedicated Ethics/ Whistleblowing Officer • Chief Compliance or Risk Officer • General Counsel/Legal Department • Human Resources department • External/independent third party • Direct disclosure to a statutory or supervisory authority
Q8	For former employees and contractors, indicate any policy limitations compared with current employees. (Select all limitations that apply)	• Limited Reporting Channels • Limited Reportable Issues • Limited Retaliation Protection • No Limitations For each, specify whether the limitation applies to: • Former employees • Contractors	• Limited Reporting Channels: Former employees • Some channels, such as speaking to your current HR representative, are inherently available only to current employees.			• No Limitations: Former employees • No Limitations: Contractors	• Limited Reporting Channels: Former employees • Limited Reporting Channels: Contractors
Q9	Which of the following best describes the anonymity and confidentiality provisions in your whistleblowing policy? (Select the one that fits best)	• Our policy does not provide for anonymous reporting • Our policy allows anonymous reporting but does not specify technical measures to protect reporter identity • Our policy allows anonymous reporting with specific technical measures in place to protect reporter identity (e.g., anonymous hotline, encrypted system) • Our policy allows anonymous reporting with technical protections AND includes confidentiality commitments for non-anonymous reports	Our policy allows anonymous reporting with technical protections AND includes confidentiality commitments for non-anonymous reports	Our policy allows anonymous reporting but does not specify technical measures to protect reporter identity		Our policy allows anonymous reporting with technical protections AND includes confidentiality commitments for non-anonymous reports	Our policy allows anonymous reporting with specific technical measures in place to protect reporter identity (e.g., anonymous hotline, encrypted system)
Q10	Does your whistleblowing policy explicitly protect employees disclosing to external parties (e.g., regulators, accredited journalists, civil-society groups) when internal channels are unavailable, conflicted, or fail to resolve a serious concern within stated timelines? (Select one) Possible Conditions: • Imminent risk of serious harm • Management or board implicated • Reasonable fear of retaliation • Internal investigation deadlines missed • Unconditional reporting to a competent regulatory authority • After internal reporting has been attempted	• No – external disclosure is not explicitly protected or is discouraged (skips follow-up question) • Limited – protected only under specific conditions (choose below) • Full – broadly protected under all listed conditions above (skips follow-up question)	Full – broadly protected under all listed conditions above (skips follow-up question) Note: Our policy specifically protects disclosures to any “national, federal, state or local agency charged with the enforcement of any laws or regulations.”	Limited – protected only under specific conditions (choose below)		Full – broadly protected under all listed conditions above (skips follow-up question)	Full – broadly protected under all listed conditions above (skips follow-up question)
Q11	If “Limited”, under which circumstances is external disclosure protected?	• Imminent risk of serious harm • Management or board implicated • Reasonable fear of retaliation • Internal investigation deadlines missed • Unconditional reporting to a competent regulatory authority • After internal reporting has been attempted • Other (specify):		Unconditional reporting to a competent regulatory authority			
Q12	Which mechanisms ensure that your whistleblowing function has access to adequate (technical) expertise to investigate reports? (Select all that apply)	• Dedicated AI experts within the whistleblowing function itself • Authority to consult internal AI experts under confidentiality safeguards, including procedures that shield case details where necessary • Standing agreements with external independent AI ethics/safety consultants • Budget authority to engage external AI experts without requiring management approval • None of the above • Other (please specify):	• Authority to consult internal AI experts under confidentiality safeguards, including procedures that shield case details where necessary				• Dedicated AI experts within the whistleblowing function itself • Authority to consult internal AI experts under confidentiality safeguards, including procedures that shield case details where necessary • Budget authority to engage external AI experts without requiring management approval
Q13	Investigation timelines and escalation rights: Which best describes your policy's commitments? (Select one)	• None – no specific timelines for acknowledgment, updates, or resolution • Basic – acknowledgment receipt ≤ 7 days only • Standard – acknowledgment ≤ 7 days and provide updates ≤ 30 days • Full – acknowledgment ≤ 7 days, updates ≤ 30 days, final outcome ≤ 90 days • Full + internal escalation – all Full timeframes plus whistleblowers may escalate to board/leadership if deadlines are missed • Full + comprehensive escalation – all Full timeframes plus whistleblowers may escalate both internally AND to regulators/external parties if deadlines are missed	None – no specific timelines for acknowledgment, updates, or resolution	None – no specific timelines for acknowledgment, updates, or resolution			Full + comprehensive escalation – all Full timeframes plus whistleblowers may escalate both internally AND to regulators/ external parties if deadlines are missed
Q14	Which specific forms of retaliation are explicitly prohibited in your policy? (Check all that apply)	• Termination/Dismissal • Demotion, or negative performance reviews • Reduction in compensation or benefits • Exclusion from meetings or information • Harassment or creating a hostile work environment • Blacklisting within the industry • Legal action against the whistleblower • None of the above	Our policy forbids retaliation. Notwithstanding the way this question is worded, it is well established under relevant law that retaliation can include termination or dismissal, demotion or negative performance reviews, or reduction in compensation or benefits. These are all covered under our policy's prohibition of retaliation. Our policy also expressly addresses harassment.	None of the above			• Termination/Dismissal • Demotion, or negative performance reviews • Reduction in compensation or benefits • Exclusion from meetings or information • Harassment or creating a hostile work environment • Blacklisting within the industry • Legal action against the whistleblower
Q15	Do any employment-, separation-, or settlement-related agreements used by your company contain non-disparagement or confidentiality clauses that could deter current or former employees from disclosing AI safety or risk-related concerns? (Select one)	• No - we do not include such restrictions in our agreements • Yes, but clauses only limit public disclosure; internal or regulator disclosures are explicitly unrestricted. • Yes, but not enforced – clauses exist, but the company has a written policy never to enforce (or threaten to enforce) them against AI safety or risk-related disclosures (no withholding of pay/equity and no legal action). • Yes, enforced - our standard confidentiality and non-disparagement provisions may restrict raising AI safety or risk-related concerns	Yes, but clauses only limit public disclosure; internal or regulator disclosures are explicitly unrestricted. We have confidentiality clauses that could impact some forms of public disclosure, but these have carveouts for internal or regulator disclosures. We do not have non-disparagement clauses in any such agreements, except in specific cases where an employee or former employee has entered a mutual non-disparagement agreement with the company.			No - we do not include such restrictions in our agreements	Yes, but clauses only limit public disclosure; internal or regulator disclosures are explicitly unrestricted.
Q16	Which anti-retaliation provisions are explicitly detailed in your whistleblowing policy? (Select all that apply)	• Defined disciplinary consequences for individuals who retaliate against whistleblowers (e.g., termination, demotion, or other concrete penalties - not just general statements prohibiting retaliation) • Documented investigation procedure for retaliation claims (including designated investigators, timelines, evidence standards, and appeal rights) • Concrete remedial measures for whistleblowers who experience retaliation (e.g., compensation, reinstatement, transfer options, or other specific remedies - not just general commitments to address retaliation) • None of the above are specifically detailed	Defined disciplinary consequences for individuals who retaliate against whistleblowers (e.g., termination, demotion, or other concrete penalties - not just general statements prohibiting retaliation)	None of the above are specifically detailed		Defined disciplinary consequences for individuals who retaliate against whistleblowers (e.g., termination, demotion, or other concrete penalties - not just general statements prohibiting retaliation) Documented investigation procedure for retaliation claims (including designated investigators, timelines, evidence standards, and appeal rights)	Defined disciplinary consequences for individuals who retaliate against whistleblowers (e.g., termination, demotion, or other concrete penalties - not just general statements prohibiting retaliation) Documented investigation procedure for retaliation claims (including designated investigators, timelines, evidence standards, and appeal rights)