Titles:	Descriptions:	Anthropic	DeepSeek	Google DeepMind	Meta	OpenAI	x.AI	Zhipu AI	ISO 37002 "gold standard"
Overall average		2.44	0	1.54	2.44	3.56	2.32	0	8.35
1. Reporting Channels, Access, and Coverage		2.6	0	4.9	5.1	6.3	1.8	0	9.5
1.1 Protected Persons Coverage	Policy should at least cover current and former employees, contractors, shareholders, suppliers, former/prospective employees, and facilitators of reports	2	0	3	2	3	2	0	10
1.2 Policy Accessibility	Policy is easily accessible to all covered persons	0	0	2	8	8	0	0	10
1.3 External Reporting Information & Rights	Policy must provide clear information about external reporting channels and the right to approach these independently of internal processes, and explain or at least link to whistleblower protection rights	0	0	5	5	7	3	0	9
1.4 Multiple Reporting Channels	Offer multiple channels for reporting misconduct internally, incl. written, oral, and in-person	5	0	9	9	7	2	0	10
1.5 Anonymous Two-Way Reporting	The system enables fully anonymous reporting with secure two-way communication between the reporter and the investigators	4	0	5	9	10	0	0	9
1.6 Ombudsperson Channel	The reporting channel is operated by an outsourced whistleblowing service provider.	0	0	0	0	3	0	0	10
1.7 Executive Oversight Channel	A separate reporting channel is available for reports concerning senior executives (e.g., direct reporting line to the board audit committee) or board members	7	0	10	3	5	0	0	8
1.8 Broad but clear material scope	Material scope covers, at a minimum, potential violations of law and, code of conduct. Ideally, also further, broad categories, while retaining a high degree of clarity of what is in and out of scope.	3	0	5	5	7	7	0	10
2. Whistleblower Protections & Anti-Retaliation Measures		1.3	0	1.3	2.9	4	3.4	0	8.3
2.1 Confidentiality Protection	Strict protection is required for the reporter's identity and any third parties mentioned in reports	0	0	2	10	8	0	0	10
2.2 Public Disclosure Protection	Protection for responsible media disclosure if internal and regulatory channels have failed or if there is an imminent or manifest danger to the public interest	0	0	0	0	0	0	0	3
2.3 List of Prohibited Practices and Anti-Retaliation Provisions	Policy must list comprehensive prohibited retaliatory actions with specific examples (demotion, harassment, termination, etc.), and explicit anti-retaliation provisions	2	0	2	2	2	5	4	0
2.4 Post-Investigation Monitoring	Active monitoring for retaliation continues for a minimum of 12 months after the investigation concludes	0	0	0	0	0	0	0	8
2.5 NDA/Non-Disparagement Exceptions	Explicit statement that NDAs and non-disparagement agreements cannot prevent safety-related whistleblowing	7	0	0	0	7	10	0	10
2.6 Good Faith or Reasonable Cause Provisions	Clear good faith or reasonable cause standard that protects honest mistakes; high burden of proof required for false report sanctions	0	0	5	8	8	10	0	10
2.7 Handler/Investigator Protection	Explicit protections for employees who receive, investigate, or support whistleblowing reports	0	0	0	0	0	0	0	8
3. Investigation Process & Standards		0.8	0	1	3.2	2.2	0.4	0	7.6
3.1 Designated Impartial Receiver	A provably independent person or department must be designated to receive and handle reports, ideally attached to the board	4	0	5	6	6	2	0	9
3.2 Seven-Day Acknowledgment	Written confirmation of report receipt must be provided within 7 days	0	0	0	10	0	0	0	10
3.3 Three-Month Feedback Timeline	Investigation status and follow-up measures must be communicated to the reporter within 3 months	0	0	0	0	0	0	0	6
3.4 Adequately Resourced Investigation Teams	Investigators must be independent from implicated departments and possess appropriate technical expertise for AI safety issues, as well as sufficient resources to investigate effectively	0	0	0	0	5	0	0	9
3.5 Investigation Appeal Process	Formal right to appeal investigation outcomes to an independent review body or board committee	0	0	0	0	0	0	0	4
4. System Governance & Quality Assurance		3	0	0	1	1	0	0	8
4.1 Comprehensive Effectiveness Metrics	Regular measurement tracking report outcomes, investigation timeliness, appeal rates, % of anonymous reports, retaliation incidents, and reporter satisfaction - not just volume	7	0	0	0	0	0	0	10
4.2 Data Retention and Deletion Policy	Clear policy specifying retention periods for reports and investigations (typically 5-7 years), secure deletion procedures, and data minimization principles	0	0	0	0	0	0	0	8
4.3 Secure Documentation System	Comprehensive audit trail with secure case management system and defined retention policies	0	0	0	5	5	0	0	9
4.4 Comprehensive Training Programs	Regular, role-specific training is provided for all employees, specialized training for managers and investigators, ideally measuring training effectiveness.	0	0	0	0	0	0	0	10
4.5 Independent System Certification	Regular third-party audit and certification of the whistleblowing system's effectiveness and compliance	8	0	0	0	0	0	0	3
5. AI Safety-Specific Provisions		4.5	0	0.5	0	4.3	6	0	N/A
5.1 AI Safety Commitment Protection	Explicit protection for reporting violations of frontier safety frameworks (e.g., RSP, Preparedness Frameworks), public AI safety commitments, and internal safety policies	8	0	0	0	5	5	0	
5.2 AI Safety Coordination	Protection for AI risk reporting to dedicated AI safety bodies (UK AI Security Institutes, US Center for AI Standards and Innovation, or other international regulatory bodies)	0	0	0	0	2	2	0	
5.3 AI risk transparency	Protections for reporting intentional deception of external evaluators, regulators, or the public, suppression of publication of safety evaluation results, and inadequate disclosure of risk to regulators and the public.	5	0	0	0	5	10	0	
5.4 Adequacy of AI risk management and cybersecurity	Protections for reporting inadequate risk management processes, incl. assessment, monitoring, mitigation, deployment pressure despite concerning levels of risk, insufficient operational and cybersecurity practices, incl. incidents	5	0	2	0	5	7	0	