GAISB

GLOBAL AI STANDARDS BODY

EDITION 1.0 / 2026

EFFECTIVE 01 Q2 2026

BINDING ON ALL CAIS HOLDERS

THE PROFESSIONAL STANDARDS LIBRARY — VOLUME II

The *CAIS* Professional Code of Conduct

The ethical, professional, and disciplinary framework governing every Certified Artificial Intelligence Strategist — worldwide, without exception.

ISSUED UNDER ISO/IEC 17024 PRINCIPLES

Adherence required for certification and renewal

GOVERNED BY THE GAISB STANDARDS COUNCIL

RATIFIED BY THE ETHICS REVIEW BOARD

Pro Bono Publico

FOR THE PUBLIC GOOD

DOCUMENT CONTROL · RATIFICATION

Document Control

The Certified Artificial Intelligence Strategist Professional Code of Conduct is a controlled normative document issued and maintained by the Global AI Standards Body. Its authority derives from the GAISB Charter and the Board-ratified Standards Development Procedure.

Document Title	CAIS Professional Code of Conduct
Edition	1.0
Document Number	GAISB-PSL-II-2026-001
Effective Date	Q2 2026
Supersedes	None — Initial Issuance
Next Scheduled Review	Q2 2029 (triennial) or earlier upon material change in normative references
Custodian	GAISB Standards Council
Approving Authority	GAISB Board of Directors, on recommendation of the Ethics Review Board
Distribution	Public document — cite with attribution
Classification	Normative · Binding on all CAIS credential holders

RATIFICATION

This Code was adopted by resolution of the GAISB Board of Directors and published under seal of the Standards Council. It takes effect on the Effective Date above and remains in force until amended or superseded.

CHAIR, GAISB BOARD OF DIRECTORS

CHAIR, STANDARDS COUNCIL

CHAIR, ETHICS REVIEW BOARD

DATE OF RATIFICATION

NORMATIVE FRAMEWORK · AUTHORITY

Normative References

The following documents constitute the normative framework against which this Code is drafted, interpreted, and enforced. Where a provision of this Code is ambiguous, the referenced instruments shall guide interpretation, with priority given to the most protective standard for affected persons.

PERSONNEL CERTIFICATION

- **ISO/IEC 17024:2012** — Conformity assessment — General requirements for bodies operating certification of persons. Basis for the certification scheme, disciplinary procedures, and appeals process described in Articles XII and XIII.

AI MANAGEMENT AND RISK

- **ISO/IEC 42001:2023** — Information technology — Artificial intelligence — Management system. Organizational counterpart to the personnel duties established in Article V.
- **ISO/IEC 23894:2023** — Artificial intelligence — Guidance on risk management. Informs the risk-assessment obligations in § 5.1 and § 5.8.
- **ISO/IEC 22989:2022** — Artificial intelligence — Concepts and terminology. Primary authority for defined terms in Appendix A.

GOVERNANCE AND ETHICS

- **NIST AI Risk Management Framework 1.0** (U.S. Department of Commerce, 2023) — Informs the Govern, Map, Measure, Manage lifecycle expectations underlying Articles III and V.
- **OECD AI Principles** (2019, updated 2024) — Informs duties of transparency, accountability, and human-centered values.
- **UNESCO Recommendation on the Ethics of Artificial Intelligence** (2021) — Informs duties to human dignity, non-discrimination, and the protection of vulnerable populations in Articles III and V.
- **UN Guiding Principles on Business and Human Rights** (2011) — Informs the duty of care to affected persons and the duty to refuse work incompatible with human rights.

ORDER OF PRECEDENCE

Where this Code, the normative references, and applicable law appear to impose conflicting obligations, the standard most protective of affected persons shall govern, subject to § 1.7 (Conflict with Law).

PREAMBLE · THE MORAL FOUNDATION

Preamble

DECLARATION OF PURPOSE

Artificial intelligence now shapes the decisions that determine who is hired, who is lent money, who receives care, who is heard, and who is seen. The design, deployment, and governance of these systems carries moral weight that cannot be delegated to institutions alone. It rests, finally, on the shoulders of the individual professionals who build, deploy, and operate them.

This Code exists because competence without conscience is dangerous, and conscience without standards is sentiment. A profession is the union of the two: documented skill bound to documented duty. The Certified Artificial Intelligence Strategist credential is extended only to those who accept both.

By certification, every CAIS accepts a public trust. This document defines that trust, the obligations it imposes, and the consequences of breaking it.

THE PROFESSIONAL COMPACT

A CAIS does not merely know how AI works. A CAIS accepts that knowing how it works creates a duty concerning how it is used. The Global AI Standards Body certifies professionals who hold that duty seriously — and disciplines those who do not.

THE BINDING NATURE OF THIS CODE

Adherence to this Code is not aspirational. It is a condition of certification. Every holder of the CAIS credential is required to attest to this Code at initial certification, at each recertification, and whenever the Code is materially revised. Violations are subject to formal disciplinary process under Article XII.

INTERPRETATION

Where any provision of this Code is ambiguous, it shall be interpreted in favor of the safety, dignity, and autonomy of persons affected by the AI systems a CAIS designs, deploys, or governs.

TABLE OF CONTENTS

Contents

FRONT MATTER

ARTICLES

APPENDICES

ARTICLE I

Scope, Applicability, and Authority

§ 1.1 Application

This Code applies to every individual who holds, has held, or is pursuing certification as a Certified Artificial Intelligence Strategist (CAIS) issued by the Global AI Standards Body (GAISB). It applies in all professional contexts, regardless of jurisdiction, employer, industry, or client.

§ 1.2 Temporal Scope

This Code applies to conduct occurring after the effective date of certification and for the duration of credential-holding. It also applies to conduct undertaken during the certification candidacy period and to any material misrepresentation made during the certification process.

§ 1.3 Extraterritorial Reach

The obligations set forth in this Code are binding on CAIS holders regardless of the jurisdiction in which they reside or practice. Where local law conflicts with a provision of this Code, the CAIS shall comply with the law and, where possible, also satisfy the spirit of the Code. Where a CAIS operates in a jurisdiction that imposes obligations exceeding those of this Code, the stricter obligation governs.

§ 1.4 Relationship to Other Standards

This Code is issued under the principles of ISO/IEC 17024 governing bodies that certify persons. It complements, but does not replace, any code of conduct imposed by a CAIS's employer, professional association, licensing authority, or the jurisdiction in which they practice. Compliance with this Code does not relieve a CAIS of any other applicable legal or professional obligation.

§ 1.5 Authority of the Ethics Review Board

Interpretation, enforcement, and amendment of this Code is vested in the GAISB Ethics Review Board (the "Board"), constituted under the authority of the GAISB Standards Council. The Board's written interpretations shall be treated as binding guidance until modified by the Board or superseded by a revision of this Code.

§ 1.6 Acknowledgment of Binding Effect

By attesting to this Code, each CAIS acknowledges that the Code forms part of the contractual relationship between the CAIS and GAISB, that violations may result in disciplinary action up to and including permanent revocation of the credential, and that the CAIS has read, understood, and accepted its obligations.

§ 1.7 Conflict with Law and Order of Precedence

Where a provision of this Code directly conflicts with a mandatory obligation imposed by applicable law, the mandatory legal obligation shall prevail to the extent of the conflict. Where this Code imposes a standard of conduct that is more protective of affected persons than that required by law, the standard of this Code shall govern. A CAIS who reasonably believes that adherence to law requires departure from this Code shall document the basis for that departure and, where circumstances permit, consult the Ethics Review Board.

§ 1.8 Interpretation

This Code shall be interpreted in light of its purpose: the protection of affected persons, the integrity of the profession, and the public trust in the CAIS credential. Ambiguities shall be resolved in favor of the most protective reading consistent with the text. Formal interpretive guidance issued by the Ethics Review Board is binding on matters of application.

ARTICLE II

Foundational Principles

The following seven principles form the moral architecture of this Code. Every specific obligation set forth in subsequent Articles derives from and must be interpreted in light of these principles. Where a specific clause is silent or ambiguous, the principles shall govern.

PRINCIPLE I

Primacy of the Public Interest

Where the interests of the public and those of any employer, client, or the CAIS personally come into conflict, the interest of the public — particularly persons affected by AI systems who did not choose to be affected — shall take precedence.

PRINCIPLE II

Human Dignity and Agency

Every AI system a CAIS designs, deploys, or governs exists in service of the dignity, agency, and flourishing of the persons it touches. A CAIS shall not knowingly design or operate systems whose primary function is to degrade, deceive, manipulate, or strip agency from human beings.

PRINCIPLE III

Honesty and Integrity

A CAIS shall tell the truth about what AI systems can do, cannot do, and fail at. A CAIS shall not overstate capabilities to win work, nor understate risks to close a sale, nor conceal known failures from those who would be harmed by them.

PRINCIPLE IV

Professional Competence

A CAIS shall practice only within the boundaries of their demonstrated competence, shall maintain currency through continuing development, and shall decline or withdraw from work where competence is insufficient to protect those affected.

PRINCIPLE V

Accountability and Transparency

A CAIS accepts accountability for the AI systems they design, deploy, and operate. Accountability is not reducible to process; it requires explanation, remediation, and, where appropriate, restitution.

PRINCIPLE VI

Fairness and Non-Discrimination

A CAIS shall not design, deploy, or knowingly permit the operation of AI systems that unjustly discriminate against persons or groups on the basis of protected characteristics, nor systems that concentrate harm on those least able to resist it.

PRINCIPLE VII

Stewardship of the Profession

A CAIS shall contribute to the integrity, reputation, and continuing development of the profession, shall mentor those entering it, shall report misconduct within it, and shall not act in ways that bring disrepute upon the credential or the Body that issues it.

ARTICLE III

Duties to the Public

The public interest is the paramount concern of every CAIS. The following obligations articulate that concern in practice.

§ 3.1 Duty of Care to Affected Persons

A CAIS shall exercise reasonable care to protect the interests, rights, safety, and dignity of persons who will be affected by an AI system they design, deploy, or operate — including persons who are not clients, not users, and who did not consent to being subjects of the system.

§ 3.2 Duty to Refuse Harmful Work

A CAIS shall refuse to undertake, continue, or endorse AI work whose foreseeable use is substantially likely to cause unjust harm, including but not limited to: systems designed to facilitate unlawful discrimination, unlawful surveillance, voter or consumer manipulation through deception, the generation of non-consensual intimate imagery, disinformation campaigns targeting elections or public health, and the facilitation of weapons intended to cause mass casualties.

§ 3.3 Duty to Warn

Where a CAIS has actual knowledge that an AI system poses a substantial and credible risk of serious harm to identifiable persons or the public, and the party responsible for the system has failed or refused to act, the CAIS shall take reasonable steps to warn those at risk, the responsible authority, or the public, as circumstances require. The CAIS is not required to expose themselves to lawful retaliation inconsistent with statutory whistleblower protections but is expected to prefer disclosure over silence.

§ 3.4 Duty of Truthful Public Communication

In public statements, published content, testimony, interviews, social media, and marketing, a CAIS shall represent AI systems, capabilities, limitations, and risks truthfully. A CAIS shall not engage in deceptive marketing, inflate capability claims, or obscure known risks in public discourse concerning AI.

§ 3.5 Duty to Persons in Vulnerable Circumstances

A CAIS shall exercise heightened care in the design, deployment, and operation of AI systems affecting children, persons with cognitive impairments, patients, refugees, prisoners, and any population whose capacity to resist or seek redress is materially diminished. Obligations owed to such persons are strict and shall be interpreted in their favor.

ARTICLE IV

Duties to Clients, Employers, and Principals

The relationship between a CAIS and their client, employer, or principal is one of professional fidelity bounded by the public interest.

§ 4.1 Competent Performance

A CAIS shall deliver work that meets or exceeds the professional standards reasonably expected of a holder of the credential. A CAIS shall not accept an engagement they lack the competence to perform, nor delegate work to persons lacking the competence to perform it.

§ 4.2 Duty of Candid Counsel

A CAIS shall offer candid, professional judgment to clients, employers, and principals, including judgments the recipient may not wish to hear. A CAIS shall not suppress unfavorable findings to preserve the engagement, nor frame recommendations to conform to predetermined conclusions.

§ 4.3 Duty to Disclose Limitations

A CAIS shall disclose to the client or employer the material limitations of any AI system or approach recommended, including known failure modes, accuracy boundaries, data limitations, and the scenarios in which the system is expected to perform poorly.

§ 4.4 Duty to Escalate Concerns

Where a CAIS identifies a substantial risk concerning an AI system and reasonable efforts to address it at the working level have failed, the CAIS shall escalate the concern to an appropriate level of authority within the client, employer, or principal organization, and shall document the escalation.

§ 4.5 Boundaries of Fidelity

Fidelity to a client, employer, or principal does not extend to participation in activities that violate this Code, applicable law, or the public interest as articulated in Article III. A CAIS shall withdraw from any engagement that requires such participation.

§ 4.6 Orderly Withdrawal

Where withdrawal from an engagement is required or elected, a CAIS shall conduct the withdrawal in a manner that, consistent with this Code, minimizes harm to the client, employer, affected persons, and the public — including reasonable transition support and protection of legitimate confidences.

ARTICLE V

Duties Concerning AI Systems

The following obligations apply to the design, development, deployment, operation, and governance of AI systems by CAIS professionals.

§ 5.1 Risk Assessment

A CAIS shall conduct, or ensure the conduct of, a documented risk assessment proportionate to the scope and potential impact of any AI system they design, deploy, or materially modify. The assessment shall address foreseeable harms to affected persons, failure modes, adversarial scenarios, and the consequences of system unavailability or degradation.

§ 5.2 Human Oversight

A CAIS shall design and deploy AI systems such that meaningful human oversight is preserved appropriate to the risk level. For high-impact decisions concerning persons — including matters of employment, credit, housing, medical care, criminal justice, immigration, and child welfare — a CAIS shall ensure the system supports contestability, human review, and the ability of a competent human decision-maker to override the system.

§ 5.3 Bias Assessment and Mitigation

A CAIS shall evaluate AI systems for disparate performance and disparate impact across relevant population groups using documented, defensible methodology, shall document findings, and shall implement reasonable mitigation where material disparities are identified. A CAIS shall not represent a system as "unbiased" absent empirical evidence.

§ 5.4 Transparency and Explainability

A CAIS shall ensure that the operation of AI systems affecting persons is disclosed to those persons where disclosure is required by law or is reasonably necessary to preserve their agency. A CAIS shall support the production of explanations appropriate to the affected audience and the context of the decision.

§ 5.5 Data Integrity and Provenance

A CAIS shall use training, evaluation, and operational data for which lawful basis and, where applicable, consent have been established. A CAIS shall not knowingly use data obtained in violation of law, in material breach of stated terms, or in violation of the reasonable expectations of the persons to whom the data pertains.

§ 5.6 Security and Robustness

A CAIS shall apply reasonable and appropriate security measures to AI systems, including protection against adversarial inputs, prompt injection, model extraction, data poisoning, and the exfiltration of training data or confidential information. A CAIS shall disclose to affected parties known vulnerabilities that present material risk.

§ 5.7 Agentic and Autonomous Systems

A CAIS involved in the design or deployment of AI agents, autonomous systems, or systems that take consequential action without direct human authorization for each action shall implement documented scope limits, permissions boundaries, auditability, a reversible stop mechanism, and an accountability pathway for downstream effects.

§ 5.8 Monitoring and Lifecycle

A CAIS shall support post-deployment monitoring of AI systems proportionate to their risk, including monitoring for drift, degraded performance, emergent behavior, misuse, and evolving harm. A CAIS shall support the retirement of AI systems that can no longer be operated safely within their intended scope.

§ 5.9 Intellectual Property and Attribution

A CAIS shall respect the intellectual property rights of others in the training, deployment, and use of AI systems, shall appropriately attribute third-party work, and shall not knowingly represent machine-generated output as the unaided work of a human where such representation is material.

ARTICLE VI

Professional Integrity and Representation

§ 6.1 Truthful Representation of Credentials

A CAIS shall represent the credential truthfully in professional contexts. The credential may be referenced using the full title Certified Artificial Intelligence Strategist, the designation CAIS, and the tier earned. A CAIS shall not use the credential title after suspension or revocation, nor imply tiers or specializations not granted.

§ 6.2 Truthful Representation of Results

A CAIS shall represent the results of AI projects, systems, and analyses truthfully in all professional contexts. This includes the accurate reporting of evaluation results, success rates, failure rates, and the limitations of studies and pilots.

§ 6.3 Prohibition on Ghost-Authorship of Capability Claims

A CAIS shall not author, approve, or endorse capability claims — including technical benchmarks, performance metrics, and customer testimonials — which the CAIS knows or reasonably should know to be materially misleading.

§ 6.4 Dissemination of Research

A CAIS engaged in research or publication shall report methods and findings with sufficient fidelity that informed readers can assess and reproduce the work, shall not selectively disclose results in a manner that materially misrepresents the underlying data, and shall acknowledge contributing parties appropriately.

§ 6.5 Integrity in Certification and Assessment

A CAIS shall not cheat, assist another to cheat, or misrepresent their identity, work, or qualifications in any GAISB certification, recertification, or assessment activity. A CAIS shall not disclose secure examination content to any person.

§ 6.6 No Disrepute

A CAIS shall not engage in conduct — professional or personal — that is reasonably likely to bring substantial disrepute upon the credential, the profession, or GAISB. This provision shall not be construed to restrict lawful personal expression, advocacy, or association.

ARTICLE VII

Confidentiality and Data Ethics

§ 7.1 Duty of Confidentiality

A CAIS shall preserve the confidentiality of information entrusted to them in the course of professional engagements. Confidential information shall not be used or disclosed for the CAIS's personal advantage, the advantage of another client, or any other purpose inconsistent with the engagement for which it was entrusted.

§ 7.2 Exceptions to Confidentiality

The duty of confidentiality does not prevent disclosure where: (a) disclosure is authorized by the party to whom the duty is owed; (b) disclosure is required by law, regulation, or lawful order; (c) disclosure is necessary to prevent imminent, substantial, and credible risk of serious harm; or (d) disclosure is required to defend against a claim against the CAIS arising from the engagement.

§ 7.3 Personal Data and Privacy

A CAIS handling personal data shall apply the principles of lawful basis, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability consistent with internationally recognized data protection standards. Where a jurisdiction imposes stricter obligations, those obligations govern.

§ 7.4 Sensitive Categories of Data

A CAIS shall apply heightened care to data concerning health, biometric identifiers, genetic information, sexual orientation, religious affiliation, political opinion, immigration status, criminal history, and children. The use of such data in AI systems requires documented lawful basis, documented necessity, and documented safeguards.

§ 7.5 Model Outputs as Derivative Information

A CAIS shall treat the outputs of AI systems trained on or prompted with confidential information as potentially confidential themselves, and shall implement appropriate controls against the inadvertent disclosure of confidential information through model outputs.

§ 7.6 Post-Engagement Obligations

Obligations of confidentiality survive the termination of the engagement and the termination of the CAIS credential, except where the information becomes lawfully public through no breach by the CAIS.

ARTICLE VIII

Prohibited Conduct

The following categories of conduct are prohibited absolutely. Violation of any provision of this Article constitutes grounds for the most severe disciplinary sanction available under Article XII.

CATEGORY 1 — AGAINST PERSONS

- Designing, deploying, or knowingly operating AI systems intended to facilitate the generation of child sexual abuse material or non-consensual intimate imagery.
- Designing or deploying AI systems whose primary purpose is to impersonate a specific real person for the purpose of fraud, defamation, or to subvert the agency of that person.
- Designing or deploying AI systems intended to facilitate unlawful discrimination, unlawful surveillance of populations protected by international human rights law, or the suppression of political speech under color of law.

CATEGORY 2 — AGAINST SAFETY

- Knowingly contributing to the design or deployment of AI systems intended to facilitate the development, acquisition, or deployment of weapons of mass destruction.
- Knowingly disabling, degrading, or circumventing safety controls on AI systems for purposes inconsistent with this Code.
- Concealing known, material, and actionable safety defects in AI systems affecting persons from parties responsible for their mitigation.

CATEGORY 3 — AGAINST INTEGRITY

- Falsifying the credentials, qualifications, or certification status of oneself or another, including misrepresentation of CAIS tier or currency.
- Fabricating, falsifying, or materially misrepresenting research results, evaluation outcomes, or capability benchmarks.
- Participating in cheating, proxy testing, or the unauthorized disclosure of secure examination content.

CATEGORY 4 — AGAINST TRUST

- Accepting or providing undisclosed compensation in connection with the recommendation, endorsement, or procurement of AI systems.
- Using confidential information entrusted in the course of one engagement for the benefit of another client, the CAIS personally, or a related party.
- Retaliating against any person for making a good-faith report of a Code violation under Article IX.

ARTICLE IX

Duty to Report and Whistleblower Protections

§ 9.1 Affirmative Duty to Report

A CAIS who acquires actual knowledge of conduct by another CAIS that constitutes a substantial violation of this Code shall, absent countervailing legal obligation, report the conduct to the Ethics Review Board within a reasonable period. The obligation is heightened where the conduct endangers persons, the public, or the integrity of the profession.

§ 9.2 Protected Disclosure

No adverse action may be taken against any person — CAIS or otherwise — for making a good-faith report of a Code violation or for cooperating in an investigation under Article XII. Retaliation against a reporter constitutes an independent violation of this Code under Article VIII § 4.

§ 9.3 Confidentiality of Reports

The identity of persons making reports in good faith shall be protected to the fullest extent consistent with due process and applicable law. Disclosure of reporter identity shall be limited to those within the investigation and adjudication process with a bona fide need to know.

§ 9.4 Channels for Reporting

Reports may be made through the GAISB Ethics Review Board's designated intake channel, which shall be continuously available and published on the GAISB website. Anonymous reports shall be received and evaluated.

§ 9.5 Bad-Faith Reports

Reports made knowingly in bad faith for the purpose of harassment, competitive advantage, or personal vendetta constitute a violation of this Code. This provision shall not be interpreted to discourage reports made in good faith that ultimately do not result in a finding of violation.

§ 9.6 Duty to Cooperate with Lawful Authority

A CAIS shall cooperate with lawful inquiries by regulators, courts, and law-enforcement bodies acting within their jurisdiction concerning AI systems the CAIS has designed, deployed, or governed, subject to legitimate claims of privilege and lawful confidentiality obligations. Nothing in this Code shall be construed to require a CAIS to violate the law, nor to waive rights afforded by law, including the right against self-incrimination.

§ 9.7 Reporting Procedures

Reports under this Article shall be filed in accordance with the procedures set forth in Appendix B. Failure to follow stated procedure shall not, by itself, render a report defective where the substance of the report reasonably identifies the conduct, the person, and the basis for concern.

ARTICLE X

Continuing Competence and Development

§ 10.1 Duty of Currency

The pace of development in artificial intelligence places an affirmative duty of currency on every CAIS. The credential represents competence assessed at a point in time; continuing competence requires ongoing learning, practice, and engagement with the evolving state of the field.

§ 10.2 Continuing Professional Education

A CAIS shall complete Continuing Professional Education (CPE) requirements as established by the GAISB Standards Council for the maintenance of the credential. The Standards Council shall publish current requirements, accepted activity categories, and documentation standards.

§ 10.3 Practice Within Demonstrated Competence

A CAIS shall not hold themselves out as competent in a domain, technique, or technology in which their actual competence is materially lacking. Where a CAIS is engaged in work that extends beyond their demonstrated competence, the CAIS shall acquire the competence, collaborate with a competent colleague, or decline the work.

§ 10.4 Mentorship and Development of Others

A CAIS shall, to the extent reasonably practicable, contribute to the professional development of colleagues and candidates entering the profession, treating such contribution as an obligation of membership in the profession rather than a discretionary act.

§ 10.5 Honest Self-Assessment

A CAIS shall cultivate honest self-assessment of competence, shall seek feedback, and shall take corrective action where assessment reveals a gap. Certification is not evidence of omniscience.

ARTICLE XI

Conflicts of Interest

§ 11.1 Duty to Identify Conflicts

A CAIS shall exercise reasonable care to identify actual, potential, and apparent conflicts of interest in connection with professional engagements, including financial interests, personal relationships, prior or concurrent engagements, and equity or consulting positions in entities whose products the CAIS is recommending or evaluating.

§ 11.2 Duty to Disclose Conflicts

A CAIS shall disclose to affected parties, in writing where practicable, any actual or apparent conflict of interest at the earliest opportunity, and shall provide sufficient information to allow the affected parties to evaluate the conflict and determine whether the CAIS may proceed.

§ 11.3 Duty to Manage or Withdraw

Where a conflict of interest cannot be adequately managed through disclosure, informed consent, or appropriate safeguards, the CAIS shall withdraw from the engagement, the conflicting relationship, or both, as necessary to preserve professional integrity.

§ 11.4 Compensation, Referrals, and Endorsements

A CAIS shall disclose all material compensation arrangements in connection with the referral, recommendation, endorsement, or procurement of AI products and services. Undisclosed compensation for such activities is prohibited.

§ 11.5 Gifts and Inducements

A CAIS shall not solicit or accept gifts, inducements, or hospitality of material value that are reasonably likely to influence, or appear to influence, the CAIS's professional judgment. Customary business courtesies of nominal value are permitted consistent with applicable policy and law.

ARTICLE XII

Enforcement, Discipline, and Sanctions

§ 12.1 Jurisdiction of the Ethics Review Board

The GAISB Ethics Review Board holds exclusive jurisdiction over the investigation, adjudication, and disposition of alleged violations of this Code by CAIS credential holders. The Board shall operate under written procedures published by GAISB.

§ 12.2 Initiation of Proceedings

Proceedings may be initiated by a good-faith report under Article IX, by referral from a governmental or regulatory authority, or on the Board's own motion based on information reasonably believed to indicate a violation. The Board shall acknowledge receipt of reports within a reasonable period.

§ 12.3 Preliminary Review and Investigation

Upon receipt of a report, the Board shall conduct a preliminary review to determine whether, if substantiated, the conduct alleged would constitute a violation. Where preliminary review indicates a substantial question, the Board shall open a formal investigation and notify the CAIS of the allegations.

§ 12.4 Rights of the Respondent

A CAIS who is the subject of an investigation under this Article shall have the right to: timely written notice of the allegations; reasonable opportunity to respond in writing and in a hearing; the assistance of counsel at the respondent's expense; access to the material evidence relied upon; and a written decision setting forth the findings, conclusions, and sanction, if any.

§ 12.5 Standard of Proof

A finding of violation shall be supported by a preponderance of the evidence. Findings of violation of Article VIII (Prohibited Conduct) require clear and convincing evidence in light of the severity of the available sanctions.

§ 12.6 Sanctions

The Board may impose one or more of the following sanctions, proportionate to the nature, gravity, and consequences of the violation, the respondent's prior record, and aggravating or mitigating circumstances:

LEVEL	DESCRIPTION	SEVERITY
Private Admonition	A confidential written statement to the respondent identifying the conduct, the violated provisions, and corrective expectations. Not publicly disclosed.	Low
Public Reprimand	A written statement of the violation published in the GAISB Register of Disciplinary Actions, with the respondent named.	Low
Required Remediation	Mandatory completion of specified education, supervised practice, or other corrective action as a condition of continued credential-holding.	Moderate
Suspension	Temporary withdrawal of the credential for a defined period, during which use of the designation is prohibited. Reinstatement may require remediation, reassessment, or both.	Moderate
Revocation	Permanent withdrawal of the credential. The individual may be permanently barred from re-certification. Publicly disclosed in the Register.	Severe
Revocation with Referral	Revocation accompanied by referral to appropriate governmental, regulatory, or law enforcement authority where the conduct may constitute an independent violation of law.	Severe

§ 12.7 Sanction Guidelines Matrix

The following matrix establishes the presumptive sanction range for violations by severity tier. The Board shall depart from the presumptive range only upon written findings that aggravating or mitigating factors (§ 12.7(c)) justify the departure. Consistency of outcome across similar cases is a governing objective of the disciplinary process.

(a) Violation Severity Tiers

TIER	DESCRIPTION	TYPICAL ARTICLES
Tier 1 — Minor	Technical or procedural violations without evidence of harm, bad faith, or recklessness. First-instance conduct readily remediated.	Articles VI, X, XI
Tier 2 — Material	Violations involving material breach of duty, negligence, or foreseeable risk of harm to affected persons or principals, even where actual harm did not occur.	Articles III, IV, V, VII
Tier 3 — Serious	Violations involving knowing misconduct, actual harm, repeated breach, or conduct that undermines confidence in the profession.	Articles III, V, VI, IX
Tier 4 — Egregious	Any conduct enumerated in Article VIII (Prohibited Conduct); conduct involving fraud, endangerment of vulnerable persons, or knowing facilitation of unlawful harm.	Article VIII

(b) Presumptive Sanction Ranges

TIER	PRESUMPTIVE RANGE	PUBLIC DISCLOSURE
Tier 1	Private Admonition to Required Remediation	Not disclosed absent repetition
Tier 2	Public Reprimand to Suspension (up to 12 months)	Published in the Register
Tier 3	Suspension (12–36 months) to Revocation	Published in the Register
Tier 4	Revocation or Revocation with Referral	Published in the Register; notification to relevant authorities where warranted

(c) Aggravating and Mitigating Factors

Aggravating: prior disciplinary history; concealment or obstruction; harm to vulnerable persons; position of trust; pattern of conduct; retaliation against reporters; violation of Article VIII.

Mitigating: self-report prior to initiation of proceedings; full cooperation; timely remediation of harm; absence of prior discipline; reliance on reasonable professional advice; duress not amounting to excuse.

§ 12.8 Interim Measures

Where the nature of the allegations and the interests of the public or affected persons so require, the Board may impose interim measures, including interim suspension of the credential pending the conclusion of proceedings.

§ 12.9 Appeals

A respondent may appeal a final decision of the Board to the GAISB Appellate Panel on the grounds of procedural error, insufficient evidence, or manifest disproportionality of sanction. The Appellate Panel shall consist of members not involved in the original proceeding and shall issue a written decision.

§ 12.10 Register of Disciplinary Actions

GAISB shall maintain a public Register of Disciplinary Actions containing all public sanctions. The Register shall be accurate, current, and preserved indefinitely except where law requires modification or expungement.

§ 12.11 Cooperation Obligation

A CAIS shall cooperate in good faith with any investigation or proceeding under this Article. Failure to cooperate, destruction or concealment of relevant evidence, or provision of false information to the Board constitutes an independent violation of this Code subject to sanction.

ARTICLE XIII

Governance, Revisions, and Effective Date

§ 13.1 Amendment Authority

This Code may be amended only by the GAISB Standards Council upon the recommendation of the Ethics Review Board. Amendments shall be ratified by written resolution, published in full, and distributed to all CAIS credential holders.

§ 13.2 Periodic Review

This Code shall be reviewed by the Ethics Review Board not less than every three years. Review shall include consideration of developments in AI technology, law, and professional practice, and of disciplinary matters arising under the Code.

§ 13.3 Effective Date of Amendments

Amendments take effect on the date specified by the Standards Council, which shall not be less than sixty (60) days after publication, except where the Council determines that an earlier effective date is required to protect the public interest.

§ 13.4 Severability

If any provision of this Code is held unenforceable in any jurisdiction, the remaining provisions shall remain in full force and effect in that jurisdiction, and the unenforceable provision shall remain enforceable in jurisdictions where it is not so held.

§ 13.5 Language of Authority

The authoritative text of this Code is the English-language edition published by GAISB. Translations are provided for convenience. In the event of a discrepancy, the English text governs.

§ 13.6 Effective Date of Edition 1.0

This Code, Edition 1.0, is effective as of the date of ratification by the GAISB Standards Council and is binding on all persons holding or pursuing the CAIS credential from that date forward.

ARTICLE XIV

Declaration of Adherence

Every holder of the Certified Artificial Intelligence Strategist credential shall attest to the following Declaration at initial certification, at each recertification, and whenever the Code is materially revised. The Declaration is recorded and retained as part of the credential holder's permanent record with GAISB.

DECLARATION

I accept and am bound by this Code.

I, the undersigned, being a candidate for or holder of the Certified Artificial Intelligence Strategist credential issued by the Global AI Standards Body, declare and affirm that:

I have read, understood, and accept the CAIS Professional Code of Conduct in its entirety.

I recognize that the credential is a public trust, not a private advantage, and that its integrity rests on my conduct.

I accept that my professional practice of artificial intelligence is bounded, at all times, by the duties set forth in this Code, including those owed to persons I will never meet and whose dignity I have no right to diminish.

I agree to submit to the jurisdiction of the GAISB Ethics Review Board in the event of any alleged violation of this Code, to cooperate in good faith with any resulting process, and to accept the consequences of any finding lawfully made against me.

I hold this credential as a matter of professional honor. I will not use it to deceive, to harm, or to stand apart from the duties it imposes.

PRINTED NAME	CAIS CREDENTIAL NUMBER
SIGNATURE	DATE

CLOSING CHARGE

You now hold competence that most do not. With it comes a duty most do not carry. Hold both well.

APPENDIX A

Definitions and Terminology

The terms defined in this Appendix have the meanings stated when used in this Code. Where a term is not defined here, its meaning is taken from ISO/IEC 22989:2022 and, absent treatment there, from its ordinary professional usage. Defined terms appear in lowercase throughout the Code for readability.

A.1 **Affected Person**

Any natural person whose interests, rights, opportunities, or lawful expectations may be materially influenced by the output, decision, recommendation, or operation of an AI system a CAIS has designed, deployed, or governed, whether or not that person is a party to the engagement in which the system is used.

A.2 **Agentic System**

An AI system that, with limited human instruction, plans and executes sequences of actions to achieve a stated objective, including but not limited to systems that initiate external API calls, make financial or contractual commitments, or modify persistent state in digital or physical environments.

A.3 **AI System**

A machine-based system that, for explicit or implicit objectives, infers from input it receives how to generate outputs — such as predictions, content, recommendations, or decisions — that can influence physical or virtual environments. The term is construed consistently with ISO/IEC 22989 and the OECD definition.

A.4 **Conflict of Interest**

A circumstance in which a CAIS's independent professional judgment, or the appearance thereof, may reasonably be impaired by competing financial, personal, organizational, or relational interests. Both actual and reasonably perceived conflicts are within the scope of Article XI.

A.5 **Good Faith**

Honesty in belief and purpose, the absence of intent to deceive or to seek unconscionable advantage, and conduct consistent with reasonable professional standards under the circumstances known or reasonably knowable to the CAIS at the relevant time.

A.6 **High-Risk AI System**

An AI system whose foreseeable failure modes include substantial risk to life, bodily safety, fundamental rights, significant financial interests, critical infrastructure, or the functioning of democratic processes, or that operates in a domain classified as high-risk by applicable law or authoritative regulatory guidance.

A.7 **Material Harm**

Injury of a kind and degree that a reasonable person would regard as significant, including but not limited to physical injury, loss of liberty, loss of legally protected rights, substantial financial loss, material reputational damage, serious psychological harm, or the denial of opportunities in employment, credit, housing, education, healthcare, or justice.

A.8 **Material Limitation**

A constraint on the capability, reliability, safety, fairness, or appropriate use of an AI system that a reasonable professional would regard as important to the decision of a principal, user, or affected person. Materiality is judged from the perspective of the person relying on the system, not the person building it.

A.9 **Personal Data and Sensitive Categories**

Personal Data means any information relating to an identified or identifiable natural person. **Sensitive Categories** include, at minimum, data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric identifiers used for unique identification, data concerning health, data concerning sex life or sexual orientation, data concerning children, and data of a comparable protective class under applicable law.

A.10 **Principal**

The client, employer, or other person or entity to whom a CAIS owes professional duties in a given engagement. Multiple concurrent principals are possible; duties among them are governed by Article IV and Article XI.

A.11 **Professional Engagement**

Any relationship in which a CAIS provides advice, design, development, deployment, operation, audit, or governance services concerning an AI system, whether compensated or uncompensated, in an employed, contracted, consulting, advisory, board, or voluntary capacity.

A.12 **Reasonable Professional**

A hypothetical CAIS of ordinary skill and prudence acting under the circumstances known or reasonably knowable to the actor at the relevant time. The standard is objective and does not require extraordinary foresight.

A.13 **Serious Violation**

Conduct that, if proved, would fall within Tier 3 or Tier 4 of the Sanction Guidelines Matrix (§ 12.7), or any conduct enumerated in Article VIII.

A.14 **Whistleblower**

Any person who, in good faith, reports conduct reasonably believed to constitute a violation of this Code, applicable law, or a serious risk to affected persons. Whistleblowers are entitled to the protections set forth in Article IX.

APPENDIX B

Reporting Procedures and Intake

This Appendix establishes the procedures for reporting violations of this Code to the Ethics Review Board. It is issued under Article IX § 9.7 and is binding on the intake and handling of reports.

B.1 Who May Report

Reports may be submitted by any person with knowledge of conduct reasonably believed to violate this Code, including credential holders, colleagues, clients, affected persons, regulators, and members of the public. Anonymous reports are accepted but are subject to corroboration requirements before formal proceedings may commence.

B.2 Channels of Submission

Reports may be filed through any of the following channels, each of which is maintained under the supervision of the Ethics Review Board:

- The secure electronic intake portal published on the GAISB website.
- Written correspondence addressed to the Ethics Review Board at the official address of record of GAISB.
- The confidential ethics hotline operated by or on behalf of the Board, where available.

B.3 Required Contents of a Report

To enable effective preliminary review, a report should contain, to the extent known:

- The identity of the CAIS alleged to have engaged in the conduct, including credential number if known.
- A description of the conduct, including dates, locations, and affected systems or persons.
- The provision of the Code reasonably believed to have been violated, where the reporter is able to identify one.
- Any supporting documents, records, or references available to the reporter.
- The reporter's identity and contact information, unless submitted anonymously under § B.1.

Technical defects in a report shall not bar consideration where the substance reasonably identifies the conduct, the person, and the basis for concern.

B.4 Acknowledgment and Timelines

The Ethics Review Board shall acknowledge receipt of a non-anonymous report within fourteen (14) days. The Board shall complete preliminary review and determine whether to open a formal investigation within ninety (90) days of acknowledgment, subject to extension for cause documented in writing.

B.5 Confidentiality of the Process

The identity of a reporter and the contents of a report shall be treated as confidential to the extent consistent with the conduct of a fair investigation, the rights of the respondent under § 12.4, and the obligations of the Board under applicable law. Unauthorized disclosure by any person participating in the process constitutes an independent violation of this Code.

B.6 Anti-Retaliation

Retaliation against a person for making a good-faith report, or for participating in an investigation, is prohibited under Article VIII (Category 4) and Article IX § 9.3. Allegations of retaliation shall be treated as a separate matter and may proceed independently of the underlying report.

B.7 **Reports Implicating Imminent Harm**

Where a report describes conduct reasonably believed to create an imminent risk of serious harm to any person, the Board shall prioritize the matter for expedited review, shall consider interim measures under § 12.8, and may refer the matter to appropriate authorities consistent with § 9.6.

B.8 **Records and Statistics**

GAISB shall maintain records of reports received, matters opened, dispositions, and sanctions imposed, in a manner that supports public reporting of aggregate disciplinary statistics while protecting the confidentiality of individuals not subject to a public sanction.

OPERATIVE NOTE

Until the Ethics Review Board's intake portal is live, good-faith reports may be directed to *ethics@gaisb.org*. Placeholder status shall be noted on the GAISB website; no report shall be deemed defective for having been submitted during this interim period.

GAISB

The Global AI Standards Body is the governance organization issuing and maintaining the Certified Artificial Intelligence Strategist (CAIS) credential and its supporting body of normative documentation.

Competence without conscience is dangerous. Conscience without standards is sentiment. A profession is the union of the two.

GOVERNED BY THE GAISB STANDARDS COUNCIL · CITE WITH ATTRIBUTION