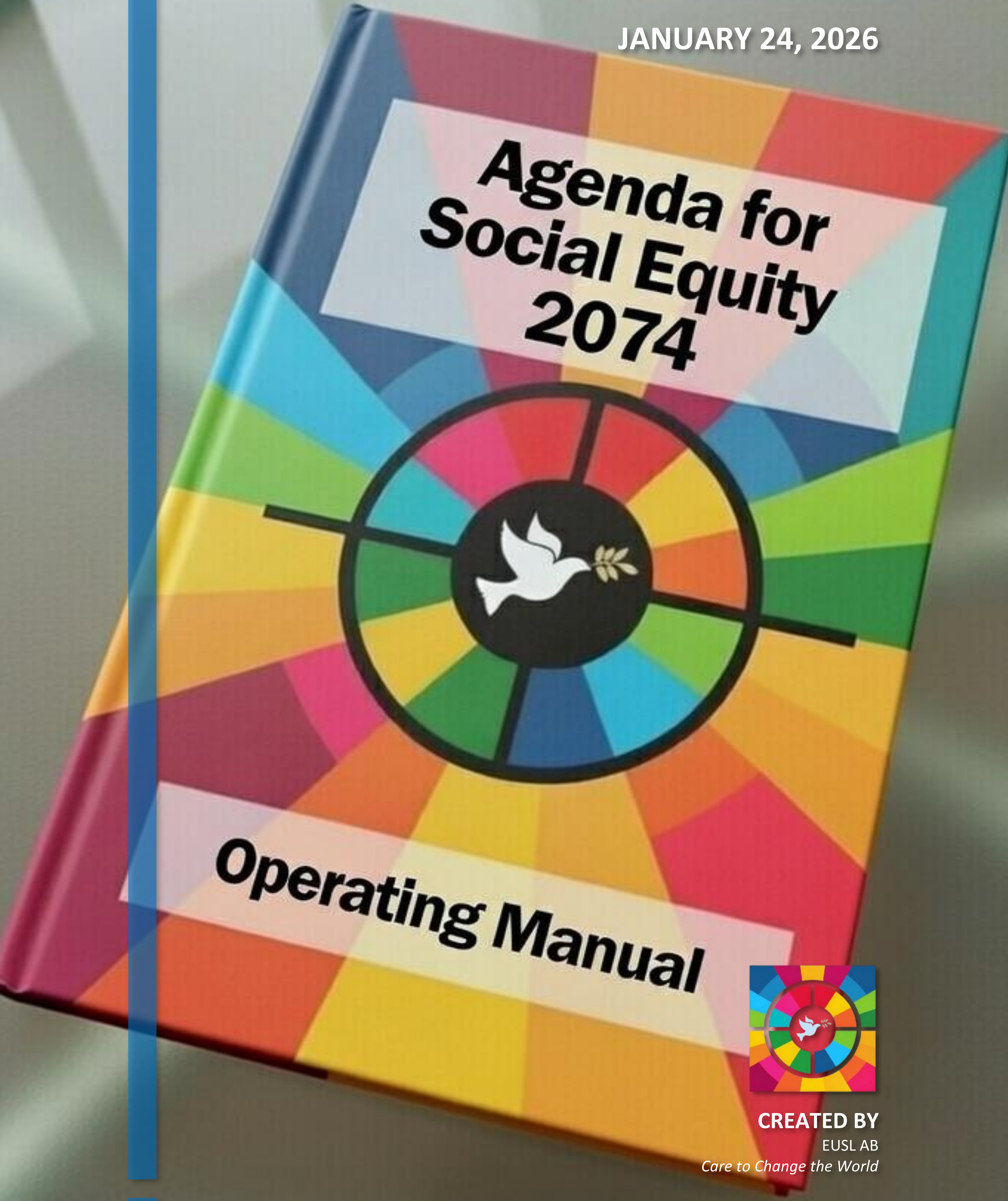
JANUARY 24, 2026



Agenda for Social Equity 2074

Operating Manual

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

Introduction 2

Chapter 1 — Open Standard Development Principles 2

Chapter 2 — Modular Design Philosophy 3

Chapter 3 — Evidence and Verification Methods 5

Chapter 4 — Progress-Based Evaluation and Proportionality 8

Chapter 5 — ISO 26000 and External Framework Alignment 10

Chapter 6 — Consent, Disclosure, and Revocation 11

Chapter 7 — Ethics Controls and Escalation 12

Chapter 8 — Periodic Review, Calibration, and Learning 14

Final Word 15

Operating Manual

Introduction

This Operating Manual constitutes the procedural and methodological backbone of the A2074-SRS ecosystem. It sets out the open-standard principles, design prerogatives, evidentiary methods, proportionality doctrine, consent architecture, ethics controls, and calibration routines that Validation Partners must observe in designing and deploying validation models. It preserves the ecosystem's defining characteristics: non-comparative evaluation, patient-level confidentiality, independence of GSIA ethics oversight, and the fair, proportionate treatment of micro-, small-, medium-, and large-scale enterprises.

The Manual must be read as an adjunct to, and consistent with, the Foundational Charter, the Rules for Interpretation of the 17 SGG Pillars, the Governance & Oversight Manual, the Digital Integration & Platform Governance Manual, the Ethics & Integrity Code, the Communication & Public Disclosure Protocol, and the Legal Compliance & International Law Note. Where provisions overlap, the strictest confidentiality rule or highest proportionality safeguard prevails.

This Manual does not prescribe a single methodology. Instead, it defines the permissible design space within which Validation Partners may innovate—stars, points, badges, levels, maturity ladders, sector modules, and deep-dive thematic models—provided such models remain aligned to the SGG canon, adhere to interpretive fidelity, protect confidentiality, and employ proportionate, least-intrusive evidence practices. The aim is methodological openness without dilution of ethical or procedural safeguards.

The Manual proceeds through eight chapters, from design principles to sunset and calibration duties, ending with a Final Word that reaffirms the open-standard doctrine and the primacy of confidentiality.

Chapter 1 — Open Standard Development Principles

This Chapter establishes the non-prescriptive design principles governing all validation models operating under A2074-SRS. These principles safeguard the freedom to innovate while ensuring that any model remains doctrinally anchored to the 17 SGG pillars, respectful of confidentiality, and compliant with GSIA oversight expectations.

An open standard is defined as a framework that:
(a) permits diverse, partner-developed methodologies;
(b) ensures interoperability across sectors and geographies;
(c) does not mandate proprietary tooling or closed-source systems;
(d) avoids monoculture by allowing multiple models to coexist; and
(e) preserves the integrity of the SGG canon and patient-level confidentiality.

All validation models must therefore satisfy five foundational criteria: Substantive Anchoring, Interpretive Fidelity, Confidentiality-by-Design, Proportionality, and Non-Comparative Operation.

Substantive Anchoring
Each model must map directly to the content and intent of the 17 SGG pillars, drawing from the Rules for Interpretation's structure of purpose, scope, examples, tests, safeguards, and sector-specific

nuances. Anchoring prevents models from drifting into unrelated ESG or commercial standards and preserves doctrinal coherence.

Interpretive Fidelity
Models must apply the interpretive rules faithfully. They may add granularity—sector modules, context-specific nuance—provided they do not alter meaning, create implied obligations, or diminish protections afforded by the Rules for Interpretation. In any tension, the Rules for Interpretation prevail.

Confidentiality-by-Design
Validation models must incorporate confidentiality into their architecture, including redaction defaults, secure evidence flows, consent governance, "view-only" enclaves, and data minimisation. Consent must be layered, explicit, informed, revocable, and logged cryptographically.

Proportionality
Models must account for enterprise size, maturity, risk profile, and sectoral exposure. Scoring or recognition mechanisms must not privilege scale over intent or effort. Microenterprises and large corporations must be able to achieve meaningful outcomes without distortion.

Non-Comparative Operation
Model outputs must not be used, marketed, or understood as comparative ratings, rankings, or competitive benchmarking. Outcomes reflect alignment with SGG standards, not superiority relative to peers.

Table 1: Open Standard Principles and Operational Implications

Principle	Operational Requirement	Oversight Mechanism
Substantive Anchoring	Model maps directly to each applicable SGG pillar	GSIA monitoring; Agenda 2074 interpretive review
Interpretive Fidelity	No alteration of pillar meaning or scope	Interpretive Notes; crosswalk checks
Confidentiality-by-Design	Secure enclaves; layered consent; minimisation	GSIA privacy audits; consent ledger verification
Proportionality	Scale-adjusted criteria; burden minimisation	Partner attestations; thematic audits
Non-Comparative Operation	No benchmarking or implicit ranking	GSIA enforcement; publication controls

Chapter 2 — Modular Design Philosophy

This Chapter articulates the philosophy of modularity that underpins the A2074-SRS operating space. Modularity allows diverse evaluation models—stars, points, badges, maturity ladders, sector modules, and deep dives—to coexist and serve different user needs while remaining interoperable and governed by the same interpretive rules and ethical constraints.

Rationale for Modularity

Modularity promotes flexibility, scalability, accessibility, and context-appropriateness. It allows enterprises to engage with the Standard at different levels of ambition and readiness, whether through lightweight badges, structured star models, granular points-based systems, or advanced maturity ladders. It ensures that no single model becomes hegemonic or exclusionary.

Permissible Model Types

The ecosystem recognizes the following model families, all of which must operate within the Rules for Interpretation and confidentiality architecture:

Stars-based Models

Structured in tiers (e.g., 1–5 stars), reflecting increasing depth of alignment with the SGG pillars. They are hospitality-inspired, intuitive, and particularly suited to broad public communication—subject to consent and non-comparative framing.

Points-based Systems

Accumulate evidence of practice, governance, and outcomes across pillars. They require clear weighting logic, justified through interpretive fidelity and proportionality.

Badges & Micro-Recognition Units

Provide focused recognition for specific SGG domains (e.g., "SGG4 Literacy Badge," "SGG11 Circularity Badge"). These models rely on deep domain specificity and are valuable for incremental or thematic engagement.

Maturity Models & Ladders

Define progressive stages (e.g., Emerging → Established → Leading) across governance, processes, and safeguards, reflecting organisational advancement. They must avoid comparisons across entities and focus solely on internal progression.

Deep-Dive Pillar Models

Offer rigorous evaluation of a single SGG pillar, often involving sector experts, advanced methodologies, and higher evidentiary thresholds.

Sector Modules

Adapt evidence expectations to sector realities while maintaining interpretive fidelity. They are advisory to all model families and cannot override SGG content.

Table 2: Modular Model Types and Characteristics

Model Type	**Primary Use**	**Evidentiary Depth**	**Strengths**	**Confidentiality Considerations**
Stars	Holistic public-facing recognition	Medium	Accessible; intuitive	Explicit consent for publication

Points	Detailed multi-pillar assessment	Medium-High	Transparent weighting; granular	Handling of weighted evidence under minimisation
Badges	Focused recognition	Low-Medium	Thematic; scalable	Narrow scope reduces exposure risk
Maturity	Organisational development	High	Longitudinal growth	Requires safeguards for historical data
Deep-Dive	Pillar-specific rigor	Very High	Expert-driven depth	Enclave-based evidence review
Sector Modules	Contextual adaptation	Variable	Tailored to sector	Must avoid re-identification through sector granularity

Internal Coherence and Cross-Model Interoperability

While models differ in structure, each must maintain internal coherence and contribute to a larger interoperable ecosystem. This requires:

(a) consistent mapping to the same set of SGG interpretive rules;
(b) alignment with cross-cutting safeguards (confidentiality, COI, AI guardrails, consent);
(c) transparent documentation of weighting, level definitions, and recognition thresholds;
(d) preservation of non-comparative framing across all external communications.

No model may require public disclosure as a condition for achieving any level or recognition. Where model design relies on public-facing recognition (e.g., star display), such display must always be voluntary, consent-based, revocable, and accompanied by non-comparative disclaimers per the Communication & Public Disclosure Protocol.

Chapter 3 — Evidence and Verification Methods

This Chapter codifies the permissible evidence types and verification methods for all validation models operating under A2074-SRS. It is governed by a least-intrusive doctrine, patient-level confidentiality, proportionality, and fidelity to the Rules for Interpretation of the 17 SGG pillars. Evidence is gathered solely to the extent necessary to substantiate claims and to operate or verify a model's determinations; any excess collection, unnecessary identity exposure, or coercive disclosure is prohibited. The methods described herein are interoperable across stars, points, badges, maturity ladders, sector modules, and single-pillar deep dives, and must be applied with clear documentation, version control, and audit-ready trails without enabling comparative ranking.

Evidence is categorised by purpose and sensitivity. Declarations and attestations are used to establish baseline representations; desk reviews verify sufficiency and coherence of submitted materials; sampling provides targeted assurance over higher-risk or material domains; field checks are reserved for proportionate, necessity-tested circumstances or explicit deep-dive requirements; and automated evidence (including digital logs) is permitted where its provenance, integrity, and privacy posture are adequately controlled. Across all methods, the consent ledger governs disclosure and use; redaction, pseudonymisation, and secure enclaves govern handling; and chain-of-custody records govern any access beyond the originating secure zone.

Declarations and attestations must be signed by accountable officers with knowledge and authority over the asserted domain, supported by policies, process descriptions, and dated artefacts sufficient to enable a reasonableness review. Desk reviews rely on structured checklists mapped to the SGG interpretive rules and the model's evidence taxonomy; reviewers are trained to recognise over-collection risks and to request clarifications without soliciting unnecessary personal data. Sampling uses risk-based criteria—materiality, control criticality, incident history, sector exposure—to determine minimal viable sample sizes and must favour redacted exemplars and metadata wherever feasible. Field checks, including remote or on-site verification, are used only when the objective cannot be achieved through less intrusive means; they must be time-boxed, scope-defined, and conducted under "view-only, no-extract" rules where sensitive artefacts are in scope.

AI-enabled verification (for example, text classification of policies or anomaly detection in consent logs) is permissible only with documented model cards, intended-use statements, bias testing and monitoring, human-in-the-loop decision points, and fallback procedures where model reliability is uncertain. No automated method may singularly determine adverse outcomes or sanctions. Third-party attestations (e.g., ISO 26000 self-declarations or vendor certifications) may be submitted as contextual evidence but cannot substitute for SGG-anchored verification nor be portrayed as A2074-SRS certification.

Table 3: Evidence types, purposes, and privacy posture

Evidence Type	**Primary Purpose**	**Typical Artefacts**	**Privacy Posture & Handling**	**Appropriate Use**
Declarations & Attestations	Establish baseline commitments and factual representations	Signed officer attestations; policy statements; governance charters	Minimal personal data; redaction by default; ledgered consent for external use	All model families as entry-level substantiation
Desk Review Materials	Verify coherence and sufficiency	Process maps; training curricula; KPI snapshots; anonymised registers	Pseudonymised where possible; secure portal submission	Core method for stars, points, badges, maturity
Targeted Samples	Test control operation and evidentiary sufficiency	Redacted case files; consent log excerpts; issue trackers	Redaction mandatory; "need-to-know" scoping; immutable access logs	Risk-based reinforcement of desk review
Field Checks (Remote/On-site)	Verify reality of controls or outcomes	Observations; interviews;	Time-boxed; view-only; no	Reserved for deep-dives or unresolved risks

		enclave-view of sensitive artefacts	extraction of identity-linked data	
Automated/Digital Evidence	Corroborate control uptime and integrity	System logs; cryptographic proofs; model monitoring dashboards	Data minimisation; provenance verification; bias monitoring	Consent ledger integrity; AI guardrail checks
Third-Party/External	Contextual corroboration	ISO 26000 self-declarations; vendor SOC reports	Referenced but not determinative; consistency checks	Supplementary only; no "certification" claims

Table 4: Verification intensity matrix (least-intrusive doctrine)

Risk/Maturity Context	Default Method Mix	Escalation Triggers	Upper Bound (with Justification)
Low Risk / Early Stage	Declarations + desk review	Material inconsistencies; KRI anomalies	Limited sampling of redacted artefacts
Moderate Risk / Growing	Declarations + desk review + targeted sampling	Repeated minor lapses; sector alerts	Remote field check under enclave rules
High Risk / Complex	Desk review + structured sampling + automated logs	Incident history; unresolved CAP items	On-site view-only verification; third-party support
Deep-Dive / Pillar-Intensive	Full method protocol incl. field elements	High materiality of potential harm	Extended enclave review with dual-control

All verification activities must be documented in working papers sufficient to enable re-performance by an independent reviewer, and yet remain rigorously minimised to avoid over-collection. Requests for identity-linked artefacts require explicit necessity tests, prior approval by an internal ethics control (as set out in Chapter 7), and adherence to secure enclave access with immutable logging and suppression of extraction. Any deviation from the least-intrusive baseline must be recorded with rationale, scope, duration, and compensating safeguards, and is subject to GSIA oversight under the Governance & Oversight Manual.

No validation outcome may be conditioned on public disclosure. Where a model contemplates public-facing recognition (for example, a consented star emblem), such recognition is always optional, revocable at will, and governed by layered consent entries that define scope, audience, and duration. Revocation must not affect the underlying private validation standing unless the model's internal logic depends on public-facing behaviour, in which case a proportionate internal alternative shall be offered.

Chapter 4 — Progress-Based Evaluation and Proportionality

This Chapter operationalises fairness through progress-based evaluation and proportionality. It ensures that entities at different capacities, sizes, and lifecycle stages can achieve meaningful recognition without being disadvantaged by scale or resource intensity, and without inducing comparative dynamics. The doctrine asserts that "everyone can do something," and that models must reflect advancement over time, not merely status at a point in time.

Progress-based evaluation requires models to articulate staged expectations, recognising foundational controls, incremental improvements, and advanced practices. Expectations must be scaled to enterprise size, sector materiality, and risk exposure. Recognition mechanisms—stars, points, badges, maturity levels—must be calibrated to reward documented progress, sustained control effectiveness, and the integrity of consent and confidentiality safeguards, rather than absolute resourcing. Where outcomes incorporate quantitative indicators, they must be normalised or context-adjusted to prevent structural bias toward larger entities.

Proportionality also governs evidentiary burden. Micro- and small-enterprises must not be required to produce the same volume or sophistication of documentation as large entities to demonstrate equivalent alignment of intent and practice; however, the integrity of confidentiality and consent controls remains non-derogable for all sizes. Sector modules may tailor expectations to operational realities (for example, the feasibility of on-site checks in dispersed micro-enterprise contexts), provided interpretive fidelity and non-comparative framing are preserved.

Models must incorporate temporal elements that recognise improvement. For maturity ladders, this entails well-defined milestones with time-bound targets and review points. For points systems, this entails awarding points for both existence and effectiveness of controls, including evidence of remedial learning captured through Corrective Action Plans. For stars, this entails criteria that reflect layered depth rather than absolute scope. For badges, this entails renewal cycles that confirm continued alignment without excessive burden.

Table 5: Proportionality levers and design safeguards

Lever	Purpose	Design Safeguard	Oversight Hook
Scale-Adjusted Criteria	Tailor expectations to size and capability	Thresholds based on headcount/turnover with caps on burden	GSIA thematic reviews for fairness
Materiality Scoping	Focus evidence where risks/impacts are greatest	Sector module maps; risk-weighted sampling	Agenda 2074 interpretive alignment
Temporal Recognition	Reward improvement over static state	Milestone-based levels; renewal cycles	Monitoring of sustained effectiveness
Burden Caps	Prevent disproportionate compliance load	Time/volume caps by size tier	Partner attestations; GSIA spot-checks

Alternative Pathways	Offer equivalent private recognition where public display is declined	Non-public badges/letters; same internal standing	Consent ledger verification; non-retaliation checks

Table 6: Illustrative size-tier calibration for evidentiary burden (minimums; stricter local law or sector logic may apply)

Size Tier (Illustrative)	**Typical Staff/Turnover**	**Baseline Evidence Set**	**Sampling Expectation**	**Field Check Expectation**
Micro	≤ 10 FTE / ≤ threshold turnover	Declarations; essential policies; minimal logs	None or very limited, redacted	Not expected absent cause or deep-dive
Small	11–50 FTE	Declarations; desk review pack; limited logs	Limited, risk-based	Remote check only if unresolved risk
Medium	51–250 FTE	Full desk review pack; control narratives; logs	Targeted sampling on critical controls	Remote or on-site only for high-risk domains
Large	> 250 FTE	Comprehensive pack; system diagrams; KRIs	Structured sampling; automated evidence	On-site for high-materiality or deep-dives

To prevent implicit comparisons, all recognition statements and artefacts must be framed as confirmations of alignment to SGG-anchored criteria at a given level or stage, without reference to peer performance or percentile ranks. Marketing materials produced by Validation Partners must include the required disclaimers under the Communication & Public Disclosure Protocol and must not condition recognition on public display or external communications.

Where an entity's context changes materially—rapid growth, sectoral shift, significant incident—the model must provide a structured pathway to re-calibrate expectations without penalising prior progress. This includes transitional grace periods, targeted remedial milestones, and the preservation of private validation continuity where public artefacts are withdrawn by consent revocation. Any recalibration must be recorded in the model's change log and, where it affects many adopters, reflected in Agenda 2074's interpretive or calibration notes.

The integrity of proportionality is verified through GSIA's assurance cycle. Monitoring and thematic audits examine whether burden caps are observed, whether evidence requests remain least-intrusive, whether small-entity pathways are substantive rather than symbolic, and whether scale-related biases are mitigated. Findings may trigger corrective action, targeted guidance, or updates to sector modules to preserve fairness. In all cases, confidentiality and consent integrity remain paramount and non-negotiable.

Chapter 5 — ISO 26000 and External Framework Alignment

This Chapter clarifies the lawful, non-misleading, and proportionate integration of ISO 26000 and other external frameworks into the A2074-SRS ecosystem. It preserves Agenda 2074's prerogative as the sole standard-setter for the 17 Social Global Goals and ensures that external frameworks may inform but never supersede, dilute, or be represented as certification under A2074-SRS. Alignment must always be interpreted through the Rules for Interpretation, the confidentiality doctrine, and the non-comparative ethos governing all validation models.

ISO 26000 is an advisory guidance standard without certification status. Validation Partners may allow entities to submit voluntary ISO 26000 self-declarations as contextual evidence. These declarations may demonstrate an organisation's internal orientation toward social responsibility, provided they do not imply or infer certification, accreditation, or formal alignment recognised by Agenda 2074 or GSIA. Validation Partners must ensure that no communication—internal, external, or promotional—suggests that ISO 26000 or any external framework is endorsed, recognised, validated, or certified within A2074-SRS.

The role of ISO 26000 within the ecosystem is contextual, supplementary, and strictly non-determinative. It may help entities articulate governance principles, stakeholder-engagement processes, or thematic approaches that support elements of certain SGG pillars. However, ISO 26000 and similar frameworks are not substitutes for SGG-anchored evidence requirements, nor do they influence scoring thresholds, star levels, maturity designations, or badge eligibility. Interpretive fidelity requires that all assessments remain grounded exclusively in the SGG pillars as defined by Agenda 2074.

External frameworks, whether thematic (e.g., child rights, circularity, biodiversity), sector-specific (e.g., agriculture, finance, extractives), or governance-oriented (e.g., anti-corruption, human rights due-diligence standards), may be referenced for clarification or background context. They serve as informational inputs rather than governing authorities. Validation Partners must document any use of external frameworks in design notes, ensuring that such use does not create conflicts with confidentiality rules, add disproportionate burdens, or induce implied obligations outside the SGG canon.

Integration of external frameworks into validation methodology requires three safeguards: interpretive alignment to prevent drift away from SGG substance; confidentiality protection to ensure that external frameworks do not require unnecessary data disclosure; and non-comparative use to ensure that frameworks do not enable benchmarking across entities. External assurance reports (e.g., SOC reports, environmental audits, or industry certifications) may supplement evidence but cannot define determinations.

All references to external frameworks must be captured in a crosswalk document that demonstrates how each referenced element aligns to, supports, or informs the relevant SGG pillar interpretation. Where conflicts arise, the Rules for Interpretation prevail absolutely.

Table 7: External Framework Alignment Requirements

Framework Type	Permitted Use	Prohibited Use	Oversight Mechanism
ISO 26000	Voluntary self-declaration; contextual evidence	Any claim of certification or A2074 endorsement	GSIA publication review; communication protocol

ESG Frameworks	Background context; optional mapping tools	Substituting SGG criteria; comparative ratings	Interpretive fidelity checks
Sector Standards	Sector modules; illustrative examples	Binding obligations outside SGG scope	Agenda 2074 standards unit review
Third-Party Certifications	Supplementary corroboration	Primary evidence; proxy certification	GSIA verification; sampling protocols

All Validation Partners must ensure clients receive written, pre-engagement notices clarifying that external frameworks—even if well-known—play a supportive role only and that the A2074-SRS outcomes remain grounded exclusively in the SGG pillars. Any deviation from these requirements constitutes a material ethical breach and may be addressed under the escalation regime in the Governance & Oversight Manual.

Chapter 6 — Consent, Disclosure, and Revocation

This Chapter constitutes one of the central safeguards of the A2074-SRS ecosystem: results are private by default, disclosure is voluntary and consent-based, and revocation of consent is a right exercisable at will. The entire consent regime is anchored in patient-level confidentiality, non-retaliation, privacy-by-design, and strict digital governance, including cryptographically verifiable consent ledgering.

All validation outcomes—stars, badges, points, maturity levels, narrative assessments, and deep-dive findings—are confidential unless the entity provides explicit, informed, granular, and revocable consent. Consent must specify the scope of disclosure, intended audiences, duration, allowed formats, and any restrictions on reuse. A single consent event does not authorise derivative or future disclosures. Consent must be recorded in the consent ledger referenced in the Digital Integration & Platform Governance Manual, capturing the date, scope, conditions, and revocation rights.

Disclosure is never a condition for validation. No Validation Partner may require public display of stars, badges, or validation outcomes as a prerequisite for participating in a model or maintaining status. Marketing incentives must be decoupled from consent decisions. Any attempt to pressure, coerce, or nudge entities into disclosure constitutes a violation of non-retaliation policy and may be addressed under GSIA’s adjudicative powers.

Revocation is an unqualified right. Entities may revoke consent at any time, without reason, and without adverse consequences to their private validation standing. Revocation triggers immediate suppression of the validation outcome from public channels and proactive withdrawal from any materials under the Partner’s control. It also triggers a compliance event requiring confirmation that revocation has been executed across all relevant digital and physical repositories. Partners must ensure that revocation does not influence the underlying private assessment unless the assessment itself required public-facing elements, in which case an equivalent non-public pathway must be provided.

Confidentiality protections extend to derived content, such as anonymised case studies or illustrative examples. Before any use of anonymised materials, Validation Partners must obtain consent where the risk of re-identification is non-negligible. If anonymisation is robust and re-identification risk is demonstrably negligible, use may proceed under the Communication & Public Disclosure Protocol with GSIA clearance. Any complaint of re-identification triggers immediate review under the whistleblowing and escalation provisions of the Governance & Oversight Manual.

Operationally, consent, disclosure, and revocation must be supported by user-friendly processes. The entity must be able to view and manage its consent status through a secure interface; initiate revocation through a simple mechanism; and receive confirmation of revocation execution, including logs of withdrawal actions taken. Consent must not be bundled, implied, or buried in general terms of service; layered notices must be used to ensure clarity.

Table 8: Consent and Disclosure Controls

Requirement	Operational Mechanism	Oversight
Explicit, informed consent	Layered notices; ledger entries; digital signature	GSIA sampling and ledger integrity tests
Private by default	No outcome displayed or shared absent consent	Monitoring of partner marketing practices
Revocation at will	Immediate suppression; withdrawal confirmation	GSIA incident checks; audit trails
Non-retaliation	Separation of commercial incentives; training	Ethics controls and adjudication chamber
Least-intrusive disclosure	Aggregated, anonymised preferred; no entity-level absent consent	Communication & Public Disclosure Protocol

Validation Partners must maintain internal policies detailing consent workflows, revocation procedures, periodic verification of ledger integrity, and staff training on non-retaliation and privacy-by-design. These policies must be auditable, version-controlled, and accessible to GSIA upon request.

This consent regime is inherent to A2074-SRS and may not be waived, diluted, or superseded by contractual arrangements, national law interpretations, or commercial preferences. Where local law requires specific disclosures, the entity must be informed in advance, and the required disclosure must be strictly limited to the statutory purpose, with separate recording in the ledger and notification to GSIA under the Legal Compliance & International Law Note.

Chapter 7 — Ethics Controls and Escalation

This Chapter sets out the internal ethics architecture that all Validation Partners must maintain to ensure that validation models are designed and operated in compliance with the ethical doctrine of the A2074-SRS ecosystem. These controls operate alongside, but remain subordinate to, GSIA's independent jurisdiction as defined in the Governance & Oversight Manual. They function as the first line of defence for safeguarding confidentiality, protecting consent, preventing conflicts of interest, ensuring integrity in evidence handling, and escalating sensitive or potentially harmful matters in a controlled, non-retaliatory manner.

Internal ethics controls must be codified in policy, supported by appropriate governance structures, and operated with demonstrable independence from commercial or marketing considerations. Each Validation Partner must establish an Ethics Control Function (ECF) with clear authority to review high-risk evidence requests, approve or deny escalations from assessors, conduct independence checks, manage conflict-of-interest declarations, and oversee the application of the least-intrusive doctrine in verification. The ECF must also maintain an internal channel for protected disclosures that complements, but does not replace, the GSIA whistleblowing mechanisms described in the Governance & Oversight Manual.

Ethics controls must be embedded in day-to-day operations. Before any assessor may request identity-linked artefacts, the ECF must approve the necessity, scope, duration, redaction plan, and secure enclave access arrangements. Before any outcome is shared externally, the ECF must verify that consent is valid, current, uncoerced, and accurately recorded in the consent ledger, and that all revocation rights are preserved. Before any conflict-sensitive domain (such as AI assessments, bias risk, or alleged workplace harm) is reviewed, the ECF must ensure that assessors have no conflicts of interest and that access will not create undue confidentiality risk.

Internal escalation processes must be designed to ensure that potential breaches are surfaced rapidly, contained immediately, and escalated to GSIA without delay where required. Matters that must be escalated include, but are not limited to: potential breaches of confidentiality; anomalies in consent ledger integrity; retaliation or perceived retaliation; misrepresentation of validation outcomes; attempts to pressure assessors; failures in enclave controls; or any concern that could materially affect trust in the Standard. Escalation to GSIA is mandatory where there is a reasonable likelihood that confidentiality, consent integrity, or fairness has been compromised.

All ethics controls must be auditable, version-controlled, and subject to periodic review. Validation Partners must maintain training programs that ensure staff understand non-retaliation, conflict-of-interest rules, confidentiality requirements, least-intrusive verification, and their duty to escalate concerns. The ECF must produce annual ethics reports for internal governance and provide redacted, anonymised summaries to GSIA as part of routine monitoring under the Governance & Oversight Manual.

Table 9: Ethics Control Functions and Escalation Pathways

Ethics Function	**Core Duty**	**Trigger for Action**	**Escalation Destination**
Conflict-of-Interest Screening	Prevent assessor bias and conflicting roles	Engagement assignment; method design changes	ECF → GSIA (if systemic)
Evidence Request Review	Ensure least-intrusive, privacy-preserving verification	Any request for identity-linked artefacts	ECF → GSIA (if breach risk)
Consent Verification	Confirm validity of disclosure and revocation rights	Any planned external communication	ECF → GSIA (if anomaly in ledger)
Internal Protected Disclosure Channel	Enable confidential reporting	Any ethics, privacy, or fairness concern raised	ECF → GSIA (for serious matters)
Ethics Training Oversight	Maintain baseline staff competence	Onboarding; annual refresh; role changes	ECF; GSIA sampling

Non-Retaliation Enforcement	Prevent punitive or chilling effects	Any reported adverse treatment	ECF → GSIA (critical breach)

Ethics controls are not a shield against accountability. Their purpose is to detect, prevent, and surface risk—not to adjudicate it. Adjudication remains within GSIA's authority. Internal ethics mechanisms must therefore remain transparent to GSIA and must neither delay nor impede external oversight. Any attempt to conceal, delay, or manage internally what must be escalated externally constitutes a material ethical breach subject to GSIA enforcement under the Governance & Oversight Manual.

Chapter 8 — Periodic Review, Calibration, and Learning

This Chapter establishes the requirements for continuous learning, iterative calibration, and periodic review across all validation models operating under A2074-SRS. These duties ensure that methodologies remain current, proportionate, and consistent with the evolving interpretation of the 17 SGG pillars, emerging evidence, sector realities, and risk patterns identified through monitoring, thematic audits, ethics casework, and stakeholder insights. Continuous learning is a structural obligation rather than a discretionary enhancement.

Validation Partners must maintain documented review cycles for each model they operate. These cycles include periodic method refreshes, calibration exercises, assessor training updates, cross-partner learning sessions, and integration of interpretive clarifications issued by Agenda 2074. The cadence of these reviews must be consistent with the complexity of the model: simpler badge-level models may require annual calibration, while complex multi-pillar frameworks or maturity ladders may require semi-annual or continuous recalibration, especially where AI-assisted components or high-sensitivity domains are involved.

Calibration ensures alignment across assessors, across models, and across Validation Partners. It must include blind sampling exercises, hypothetical case analysis, scenario comparisons, threshold testing, and consistency checks against the Rules for Interpretation. Where calibration identifies variance, Partners must implement corrective measures, retrain assessors, adjust documentation, or revise method guidance. Major variances or cross-partner inconsistencies must be escalated to GSIA, which may issue ecosystem-wide calibration notes or initiate interpretive clarifications with Agenda 2074.

Learning mechanisms must be formal and documented. Each Validation Partner must maintain a learning log that records insights from monitoring findings, thematic audits, casework outcomes, stakeholder feedback, and periodic panel advisories under the Governance & Oversight Manual. These logs serve as sources for periodic method improvements and evidence taxonomy refinements. Learning artifacts must be anonymised and must not contain identity-linked data or sensitive evidence unless required and safeguarded in accordance with the confidentiality doctrine.

Review cycles must also incorporate updates to training content, ensuring that assessors remain proficient in consent governance, enclave protocols, redaction techniques, bias mitigation, least-intrusive evidence collection, and interpretive fidelity. Where learning suggests that evidence burdens are disproportionate for certain size tiers or sectors, model adjustments must be proposed through documented change logs and submitted for GSIA review.

Table 10: Periodic Review and Calibration Requirements

Review Function	**Minimum Cadence**	**Purpose**	**Oversight Link**
Method Refresh	Annual (badge models); semi-annual (multi-pillar models)	Maintain relevance and interpretive fidelity	Agenda 2074 interpretive updates; GSIA checks
Calibration Exercise	Semi-annual	Ensure consistency across assessors and partners	GSIA thematic audits; monitoring
Assessor Training Update	Annual; more frequent for high-risk domains	Maintain competence in evidence, consent, and ethics	Ethics controls; GSIA sampling
Learning Log Integration	Continuous, reviewed quarterly	Incorporate lessons from incidents, whistleblowing, audits	GSIA casework insights
Sector Module Update	As triggered by sector change or risk	Maintain contextual accuracy	Agenda 2074 sector guidance
Change Log & Versioning	Continuous	Preserve transparency of method evolution	Governance & Oversight Manual cross-reference

All recalibrations must be captured in version-controlled change logs with clear effective dates, justification, transition periods, and crosswalks to prior versions. These logs must be shared with GSIA during monitoring cycles, and any calibration materially affecting model outcomes must also be communicated to Agenda 2074 for potential issuance of interpretive notes or sector addenda.

Learning must be shared without compromising confidentiality. Partners may contribute anonymised insights to cross-partner exchanges facilitated by GSIA or Agenda 2074, provided that no identifiable information, proprietary commercial strategy, or sensitive evidence is disclosed. GSIA may convene learning forums, calibration workshops, or sector-specific roundtables to harmonise practice across the ecosystem.

Periodic review, calibration, and learning processes are not optional. They are the constitutional mechanisms that uphold fairness, methodological integrity, and coherence across an open-standard validation landscape. Consistent implementation ensures that the Standard remains responsive to real-world developments while preserving uniformity of principle, ethical discipline, and the confidentiality-first architecture that defines A2074-SRS.

Final Word

This Operating Manual closes by reaffirming that A2074-SRS is an open, non-prescriptive standard that protects confidentiality as a first principle, preserves interpretive fidelity to the 17 SGG pillars, and enables methodological pluralism without sacrificing ethical discipline. Validation Partners remain free to design stars, points, badges, maturity ladders, sector modules, and deep-dive models, provided each model is substantively anchored to the SGG canon, operates proportionately, avoids any comparative posture, and is governed by least-intrusive evidence practices and layered, revocable consent.

Openness is a duty paired with restraint. It requires transparent documentation of method logic, evidence taxonomies, weighting rationales, and change controls, while simultaneously delimiting collection and use of data to what is strictly necessary. It requires rigorous calibration and periodic review to preserve internal coherence across assessors and external coherence across models and partners, while ensuring that microenterprises and large corporates can progress meaningfully on equitable terms. It requires respectful engagement with external frameworks, including ISO 26000, strictly as contextual inputs that never supplant SGG-anchored criteria nor infer certification or endorsement.

Confidentiality remains non-derogable. Results are private by default; any disclosure is voluntary, specific, informed, and revocable at will, recorded in a verifiable consent ledger and actioned promptly upon withdrawal. No model may condition participation or status on public display. Non-retaliation protections and privacy-by-design digital governance are operational corollaries of this doctrine; they extend to whistleblowers, assessors, clients, and affected stakeholders. Evidence handling follows minimisation, redaction, secure enclaves, immutable audit trails, and proportional access, with AI-enabled tools constrained by documented guardrails and human oversight.

Ethics controls within each Validation Partner function as the first line of defence, ensuring conflict-of-interest screening, consent verification, and escalation of sensitive matters. Oversight and adjudication remain the remit of GSIA, whose independent ethics jurisdiction is the systemic guarantor of fairness and due process. Continuous improvement is institutionalised through periodic review, cross-partner calibration, learning logs, and versioned change management. Where law or risk necessitates rapid adjustments, temporary safeguards and disciplined transition plans protect adopters while maintaining historical comparability.

This Manual is read together with the Foundational Charter, the Rules for Interpretation, the Governance & Oversight Manual, the Digital Integration & Platform Governance Manual, the Ethics & Integrity Code, the Communication & Public Disclosure Protocol, and the Legal Compliance & International Law Note. In the event of tension, the stricter confidentiality and consent provisions prevail. Nothing herein authorises ranking, benchmarking, or any representation of ISO 26000—or any other framework—as certification under A2074-SRS.

The obligations are clear and reciprocal. Validation Partners design and operate compliant, proportionate, least-intrusive models; Agenda 2074 safeguards doctrinal integrity and interpretive clarity; GSIA preserves ethical independence, remedies breaches, and verifies control effectiveness; affiliated entities contribute research, capacity, and technology under ring-fenced access and conflict controls. The public interest is served through anonymised, aggregated transparency, never through exposure of entity-level results absent explicit, revocable consent.

The Manual takes effect upon issuance and remains subject to the change governance and sunset mechanisms described herein. Its legitimacy will be measured not by the volume of disclosures or the complexity of methods, but by the quiet reliability with which it enables fair progress, protects the dignity of participants, and sustains trust.

Table: Operating Doctrine and Practical Requirements

Operating Doctrine	**Practical Requirement**	**Oversight Anchor**
Open, non-prescriptive standard	Multiple model families permitted within SGG-anchored design space	Agenda 2074 interpretive notes; GSIA monitoring
Confidentiality by default	Layered, revocable consent; secure enclaves; immutable logs	Governance & Oversight Manual; Digital Governance Manual
Proportionality and progress	Scale-adjusted criteria; burden caps; temporal recognition	GSIA thematic audits; partner change logs
Least-intrusive verification	Declarations, desk review, risk-based sampling; field checks by necessity	Ethics controls; GSIA verification protocols
Non-comparative operation	No rankings or peer benchmarks in outputs or marketing	Communication & Public Disclosure Protocol
External frameworks as context	ISO 26000 self-declaration optional and non-determinative; no certification claims	GSIA communications review
Continuous calibration and learning	Periodic review cycles; assessor calibration; anonymised learning exchange	GSIA learning forums; versioned change logs

With these commitments and controls, the Operating Manual fulfills its purpose: to guide the creation and operation of compliant validation models that are open yet disciplined, innovative yet responsible, and always faithful to confidentiality, fairness, and the substance of the 17 SGG pillars.