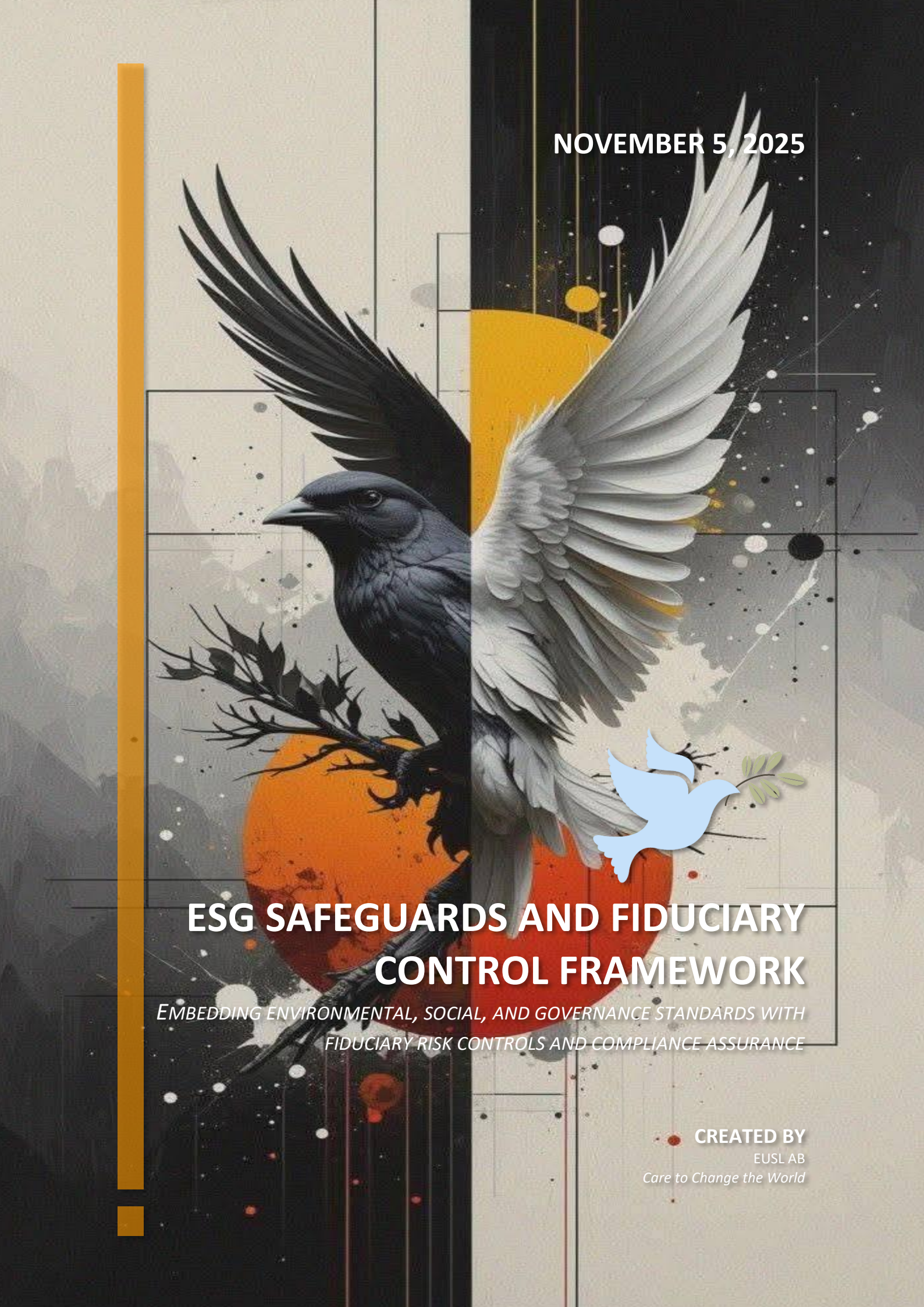

NOVEMBER 5, 2025

ESG SAFEGUARDS AND FIDUCIARY CONTROL FRAMEWORK

EMBEDDING ENVIRONMENTAL, SOCIAL, AND GOVERNANCE STANDARDS WITH FIDUCIARY RISK CONTROLS AND COMPLIANCE ASSURANCE

CREATED BY
EUSL AB
Care to Change the World

Table of Contents

ESG Safeguards and Fiduciary Control Framework

This Framework embeds environmental, social, and governance standards into GSIA operations, integrating gender and inclusion safeguards, anti-corruption measures, grievance redress mechanisms, and fiduciary risk controls. It mandates compliance monitoring and interfaces with MEL and assurance systems to uphold public-interest objectives.

Chapter 1 — Environmental and Social Standards

1.1 Purpose and scope. This Framework establishes the environmental and social (E&S) standards and controls that bind all GSIA engagements, including Flowhub Trio Plus operations under both the Standard Custodianship and Hosted Ownership variants. It applies to GSIA SCE, GSIA Holding AB, GSIA AB, EUSL-designated special-purpose vehicles, Members, Hybrid RECs, vendors, financiers, and any third party operating within a ring-fenced project perimeter. The standards herein are non-derogable unless a time-limited, reasoned exception is adopted by the competent GSIA SCE oversight organ and publicly recorded with lawful redactions.

1.2 Constitutional placement and prevalence. Environmental and social safeguards are integral to the public-interest mandate established by the GSIA Charter and the Flowhub Manual. Where a conflict arises between private instruments and these safeguards, this Framework prevails, subject only to mandatory national public law. Contractual instruments—Program Participation Agreements, SLAs, Leasing Instruments, Implementation Agreements, and procurement contracts—shall incorporate and not dilute the obligations set out in this Chapter.

1.3 Standard-setting approach. GSIA adopts a principles-and-evidence-based approach to E&S safeguards comprising: (i) binding policy standards codified herein; (ii) a risk-proportionate screening and categorisation process; (iii) due diligence and impact assessment obligations commensurate with risk; (iv) prevention, mitigation, and compensation measures embedded in project design and contracts; (v) monitoring and verification protocols aligned with MEL; and (vi) transparent publication and grievance access aligned with Chapter 4 of this Document. Localization to domestic legal frameworks is pursued without dilution; where domestic standards are more stringent, the stricter standard applies.

1.4 Screening and categorisation. Prior to approval or contracting, each project or sub-project is screened against defined E&S risk criteria and categorised by potential adverse impacts, including scope, severity, reversibility, cumulative effects, and sensitivity of affected receptors. Category determinations are reasoned and recorded, trigger proportional assessment requirements, and are disclosed with lawful redactions. Category upgrades are mandatory upon material scope changes or newly identified risks.

1.5 Impact assessment and management. Projects presenting more than minimal risk require an environmental and social impact assessment proportionate to the category, including alternatives analysis, baseline studies, and specific management plans (e.g., environmental management plans, biodiversity action plans, labour management procedures, community health and safety plans, cultural heritage management plans). Where indigenous peoples or comparable groups are affected, specialized assessments and engagement protocols are mandatory, including culturally appropriate

consultations and documented outcomes. Management plans are operational instruments, integrated into procurement and contract requirements, and monitored as performance obligations.

1.6 Pollution prevention, resource efficiency, and climate. Projects shall adopt measures that prevent, minimize, or control pollution to air, water, and land; promote resource efficiency in energy, water, and raw materials; and mitigate greenhouse gas emissions consistent with project context and proportionality. Climate risk screening is conducted to identify physical and transition risks; where material, climate-resilience measures and adaptive design requirements are incorporated in the Implementation Agreement and technical specifications. Fuel switching, energy efficiency, and circularity measures are prioritized where cost-effective and feasible without impairing service continuity.

1.7 Biodiversity and ecosystem services. Projects shall avoid critical habitat conversion or degradation. Where avoidance is not possible and the project remains necessary in the public interest, the project must: (i) demonstrate no net loss for natural habitats and net gain for critical habitats through a mitigation hierarchy; (ii) adopt biodiversity management plans; and (iii) implement offset or compensation measures only as a last resort and under verifiable, durable arrangements. Ecosystem services dependencies and impacts are identified and addressed to safeguard community livelihoods and resilience.

1.8 Community health, safety, and security. Projects shall assess and manage risks to communities arising from project activities, equipment, and infrastructure, including traffic, hazardous materials, structural safety, vector-borne disease, emergency response, and security arrangements. Security personnel engaged for project purposes shall be trained, vetted, and governed by use-of-force and conduct standards that respect human rights; complaints mechanisms must be available and effective.

1.9 Land acquisition, resettlement, and livelihoods. Involuntary resettlement is avoided wherever possible. Where unavoidable and lawful, it is minimized, and adverse impacts are mitigated through resettlement action plans that provide compensation at replacement cost, livelihood restoration, and special assistance for the vulnerable. Land acquisition and land use restrictions are conducted transparently, with meaningful consultation and access to grievance mechanisms, and are documented and published with lawful redactions.

1.10 Labour and working conditions (non-gender specific). All employers within the project perimeter—including primary contractors and significant sub-contractors—shall respect freedom of association and collective bargaining where permitted by law; prohibit forced and child labour; prevent discrimination and harassment; and provide safe and healthy working conditions, fair wages, adequate working hours, and access to grievance procedures. Occupational health and safety risks are assessed and managed; incidents are recorded, investigated, and reported under the SLA incident protocols.

1.11 Cultural heritage. Tangible and intangible cultural heritage potentially affected by projects shall be identified and protected through appropriate measures, including chance-find procedures integrated into contracts and site protocols. Engagement with affected communities over heritage of cultural significance is required, and restrictions on access are avoided unless necessary for protection or safety and accompanied by mitigation measures.

1.12 Contractualisation and enforcement. E&S obligations are integrated into procurement documents, evaluation criteria, contract conditions, change-control thresholds, and performance security requirements. Non-compliance triggers contractual remedies, including cure plans, withholdings, re-procurement, disqualification, or termination for cause, proportionate to severity and

risk. Material breaches are reportable incidents under the SLA and are escalated to the relevant committees and, where applicable, to external authorities.

1.13 Monitoring, verification, and publication. E&S performance is monitored against defined indicators, with verification by qualified personnel and, where risk-appropriate, by independent experts. Monitoring reports and corrective action plans are recorded in tamper-evident repositories and summarized for publication with lawful redactions. Lessons-learned are incorporated into adaptive management and subsequent procurements.

1.14 Interfaces. This Chapter interfaces with gender and inclusion safeguards (Chapter 2), anti-corruption and procurement integrity (Chapter 3), grievance redress (Chapter 4), fiduciary risk controls (Chapter 5), compliance monitoring (Chapter 6), the Flowhub Manual (Document 03), and the Unified MEL Framework (Document 08). Nothing herein diminishes fiduciary ring-fencing, publication duties, or the reversion covenant under Hosted Ownership.

Chapter 2 — Gender and Inclusion Safeguards

2.1 Purpose and scope. Gender and inclusion safeguards ensure that GSIA programs equitably benefit and do not adversely impact women, men, girls, boys, and persons of diverse gender identities; persons with disabilities; youth and older persons; indigenous peoples; minorities; displaced persons; and other groups facing structural barriers. The safeguards are mandatory across all Flowhub engagements and are embedded from eligibility screening to domestication, irrespective of Leasing Instrument variant.

2.2 Principles. The safeguards rest on principles of non-discrimination, equality of opportunity and outcomes, accessibility, dignity, participation, informed decision-making, and do-no-harm. They are implemented proportionately to risk and impact and are documented through verifiable evidence in the project record.

2.3 Gender and inclusion analysis. Prior to approval, each project conducts a context-specific gender and inclusion analysis that identifies: (i) differential needs, constraints, and opportunities; (ii) potential adverse impacts and barriers to access; (iii) intersecting vulnerabilities (e.g., gender-disability-poverty); and (iv) social norms or legal constraints affecting participation and benefit. The analysis informs design choices, targeting strategies, inclusive procurement specifications, and monitoring baselines and targets, and is recorded in the instrument file and disclosed with lawful redactions.

2.4 Inclusive design and accessibility. Project design incorporates accessibility standards and reasonable accommodation measures proportionate to context, including barrier-free physical access; accessible communications; inclusive digital services; and user feedback loops. Where infrastructure is involved, accessible design parameters and inspections are integrated into technical specifications and acceptance criteria.

2.5 Participation and consent. Stakeholder engagement plans ensure meaningful participation of affected and beneficiary groups, including women-led organisations, organisations of persons with disabilities, youth groups, and minority representatives. Consultations are inclusive, accessible, and culturally appropriate; their outcomes are documented and reflected in project design, contracts, and performance indicators. Where consent standards are applicable (e.g., for indigenous peoples under domestic law), the instrument incorporates procedures to seek and document such consent in good faith.

2.6 Safe access and safeguarding. Projects establish proportionate safeguarding measures to prevent sexual exploitation, abuse, and harassment, and to protect children and vulnerable adults from harm related to project activities. Requirements include codes of conduct; training; safe recruitment and vetting; accessible reporting and referral pathways; survivor-centred response; and confidentiality protocols. Contractual clauses make safeguarding a condition of contract performance, with specific remedies for violations.

2.7 Employment and economic inclusion. Procurement and contracting incorporate fair opportunity measures, such as requirements or evaluation credits for women-owned, youth-owned, disability-inclusive, or minority-owned enterprises; commitments to inclusive hiring and fair working conditions; and capacity-building for local suppliers. Targets are set contextually and monitored through verifiable evidence. Quotas may be used where lawful and justified, with publication of rationale and results.

2.8 Pricing, affordability, and service equity. Where projects deliver services to the public, tariff and pricing policies are assessed for affordability and equity, with measures to prevent exclusion of low-income or marginalized users, such as lifeline rates, targeted subsidies, phased payments, or community-based modalities. Decisions are reasoned, disclosed, and monitored for unintended consequences.

2.9 Indicators, baselines, and KPIs. Gender- and inclusion-responsive indicators and baselines are defined in the MEL framework and in the SLA KPI schedule, including participation rates, access measures, satisfaction scores disaggregated by relevant characteristics, safeguarding incident metrics, inclusive procurement shares, and employment outcomes. Disaggregation respects data-protection and minimisation principles and is accompanied by privacy-preserving publication methods.

2.10 Data protection and dignity. Collection and processing of sensitive personal data for inclusion monitoring adhere to the Data Protection and Digital Trust Policy, limiting collection to what is necessary, ensuring lawful bases, applying security controls, and protecting dignity and confidentiality. Publication employs aggregation, anonymisation, or pseudonymisation to mitigate re-identification risk.

2.11 Remedies and adaptive management. Where monitoring reveals inequitable outcomes or unintended exclusion, corrective measures are designed and implemented without delay, including design adjustments, targeted outreach, accessibility enhancements, or contractual variation. Material shortcomings trigger escalation under the SLA and may lead to re-procurement or sanctions where attributable to contractor breach.

2.12 Governance and accountability. The Ethics, Conflicts, and Investigations Committee oversees safeguarding incident pathways; the Programs and Domestication Committee monitors inclusion benchmarks linked to domestication gates; and the Data Protection and Digital Trust Committee reviews high-risk data processing. Findings and corrective actions are reported to the Executive Board and summarized for public disclosure with lawful redactions.

2.13 Interfaces. This Chapter interfaces with Environmental and Social Standards (Chapter 1), Anti-Corruption and Procurement Integrity (Chapter 3), Grievance Redress Mechanisms (Chapter 4), Fiduciary Risk Controls (Chapter 5), Compliance Monitoring (Chapter 6), the Flowhub Manual (Document 03), and the Unified MEL Framework (Document 08). It does not derogate from ring-fencing, publication, or reversion covenants established elsewhere in the GSIA corpus.

Chapter 3 — Anti-Corruption and Procurement Integrity

3.1 Purpose and scope. This Chapter establishes binding anti-corruption, ethics, and procurement-integrity obligations for all activities undertaken within the GSIA institutional perimeter, including Flowhub Trio Plus engagements under both the Standard Custodianship and Hosted Ownership variants. It governs GSIA SCE, GSIA Holding AB, GSIA AB, EUSL-designated vehicles, Members and Hybrid RECs acting as competent authorities, vendors, financiers, and any third party with access to ring-fenced assets, systems, or decision processes.

3.2 Definitions and prohibitions. Corruption, for the purposes of this Chapter, includes bribery, kickbacks, facilitation payments, undue advantage, embezzlement, misappropriation, fraud, collusion, coercive and obstructive practices, bid-rigging, and any knowing omission that has the effect of deceiving a public or GSIA authority. All such conduct is prohibited. Facilitation payments, irrespective of local custom, are prohibited unless a documented and immediate threat to life or liberty compels payment; such events are treated as incidents, recorded, and escalated with evidence and a mitigation plan.

3.3 Standards of conduct and certifications. Directors, staff, secondees, consultants, evaluators, and vendors shall comply with codes of conduct and conflict-of-interest obligations established in Document 05, Chapter 4, and with procurement-integrity rules herein. Vendors and key subcontractors provide anti-corruption certifications as conditions of contract, disclose beneficial ownership and politically exposed persons (PEPs) relationships, and commit to audit and publication clauses. False certifications or non-disclosure constitute material breach.

3.4 Procurement integrity framework. Procurement within the ring-fenced perimeter is conducted under an approved plan annexed to the SLA and Implementation Agreement, employing transparent, competitive methods proportionate to risk and value. Specifications shall be non-restrictive, evaluation criteria published, and communications with bidders recorded through defined channels. Blackout rules apply from solicitation to award and through any protest period. Change orders are controlled by thresholds and require the same evidentiary discipline and approvals as original awards.

3.5 Segregation of duties and authority controls. The authority matrix, annexed to the SLA, separates specification, evaluation, approval, and contract-administration roles. No person may influence end-to-end outcomes. Four-eyes approvals, beneficiary countersignature at defined thresholds, and immutably logged decisions are mandatory. System administrators may not act as initiators, evaluators, or approvers for the same procurement.

3.6 Due diligence and screening. Prior to award, vendors and significant subcontractors undergo integrity due diligence, including sanctions and watchlist screening, PEP checks, beneficial ownership verification, adverse media review, and conflict-of-interest screening of key personnel. Results are recorded in the contract dossier. Elevated-risk awards require enhanced diligence, including on-site verification or independent references. Ongoing monitoring is conducted for the contract duration and recorded in tamper-evident repositories.

3.7 Payment controls and value for money. Disbursements follow the payment waterfall and are contingent on verifiable delivery, documented acceptance, and, where mandated, independent verification. Advance payments require proportionate security (e.g., advance payment guarantees) and milestone-linked recovery schedules. Price reasonableness is evidenced through competition, benchmarks, or cost analysis. Any deviations are justified by reasoned note and approved at the defined escalation level.

3.8 Gifts, hospitality, and sponsorships. Gifts, hospitality, travel, sponsorships, and charitable donations related to project actors are restricted, declared, and recorded in registers per Document 05, Chapter 4. Vendors may not offer or provide such advantages to persons involved in specification, evaluation, approval, or contract administration. Sponsorships or CSR activities by vendors shall not be made contingent on procurement outcomes and require prior approval and publication.

3.9 Third-party intermediaries and agents. The use of agents, lobbyists, or intermediaries in relation to a procurement is discouraged and, where proposed, requires prior written approval, full disclosure of scope, compensation, and beneficial ownership, and enhanced diligence. Contingent fee arrangements tied to award outcomes are prohibited. Intermediary contracts are published with lawful redaction.

3.10 Red flags and incident response. Indicators of potential corruption or integrity breach—such as repetitive single-source awards without justification, unusual payment structures, undisclosed subcontracting, evaluation anomalies, last-minute specification changes, or conflicts discovered post hoc—are logged as incidents, escalated to the Procurement and Integrity Committee and the Ethics, Conflicts and Investigations Committee, and investigated under Document 11. Immediate containment measures may include suspension of award or payments, preservation of evidence, and temporary reassignment of conflicted personnel.

3.11 Investigations, cooperation, and evidence. The Ethics, Conflicts and Investigations Committee coordinates investigative steps with Internal Audit, ensuring chain-of-custody for documents, logs, and devices; secure interviews; and preservation of due process. Vendors and staff have a duty to cooperate. Non-cooperation, spoliation, or obstruction are sanctionable breaches. Where criminal conduct is reasonably suspected, referrals to competent authorities are made without prejudice to contractual remedies.

3.12 Sanctions and debarment. Proven violations trigger proportionate sanctions under the Sanctions Grid (Document 11), which may include written reprimand, removal from role, suspension of eligibility, financial penalties where lawful, termination for cause, and debarment for defined periods. Cross-debarment or recognition of reputable third-party debarment lists may be applied by reasoned resolution. Sanctions are published in summary with lawful redaction to protect ongoing investigations or legal processes.

3.13 Beneficial ownership and transparency. All prime vendors and significant subcontractors must disclose beneficial ownership and update disclosures upon changes. Disclosures form part of the public contract dossier, redacted only as strictly necessary under applicable law. Failure to disclose or misrepresentation is a material breach.

3.14 Hosted Ownership safeguards. Under Hosted Ownership, the title-holding entity shall not enter financing, security, or other arrangements that create incentives misaligned with the public-interest mandate. Any financing utilising project assets acknowledges the ring-fenced and reversionary character and prohibits private distribution. Arrangements are reviewed by the Hosted Ownership Oversight Committee prior to execution and are published with lawful redaction.

3.15 Training and attestations. All personnel participating in specification, evaluation, award, contract administration, or payment approvals complete periodic anti-corruption and procurement-integrity training and sign annual attestations. Vendors receive integrity briefings as part of kick-off and sign acknowledgement of obligations. Completion and attestations are recorded and monitored as KPIs under the SLA.

3.16 Publication, records, and auditability. Procurement plans, solicitations, award notices, material change orders, protest decisions, and sanctions are published pursuant to the transparency doctrine, with lawful redactions. Complete contract dossiers—solicitation, bids or proposals, evaluation records, approvals, contracts, guarantees, payment records, performance reports—are retained per the records schedule and made available to Internal Audit, external auditors, and oversight organs.

3.17 Interfaces. This Chapter interfaces with Document 03 (fiduciary controls, authority matrices, publication), Document 05 (committees, conflicts), Document 11 (ethics, investigations, sanctions), Document 10 (continuity incidents), and Document 12 (data protection for procurement and investigation records). Nothing herein permits dilution of ring-fencing, publication duties, or reversion covenants.

Chapter 4 — Grievance Redress Mechanisms

4.1 Purpose and scope. Grievance Redress Mechanisms (GRMs) provide accessible, predictable, and effective avenues for individuals and communities to raise concerns, seek remedy, and obtain timely responses regarding harms or risks arising from GSIA-related activities, including fiduciary, procurement, delivery, environmental, social, safeguarding, and data-protection matters. GRMs operate alongside, and do not replace, judicial or administrative remedies available under national law.

4.2 Principles. GRMs are founded on legitimacy, accessibility, predictability, equity, transparency, rights-compatibility, and continuous learning. They are survivor-centred for safeguarding matters, protect against retaliation, and respect confidentiality and privacy consistent with lawful disclosure and publication duties.

4.3 Architecture and channels. A multi-channel GRM is established for each project perimeter, comprising at minimum: a public web portal with accessible formats, toll-free phone lines where feasible, community liaison points for in-person submissions, secure mail and email options, and dedicated worker grievance channels at contractor sites. Channels accommodate multiple languages and disability accessibility needs and provide anonymous reporting options where lawful and appropriate.

4.4 Registration, acknowledgement, and triage. Grievances are registered in a tamper-evident system with unique identifiers, time-stamps, and classification (environmental/social, labour, safeguarding, fiduciary/procurement, data protection, other). Acknowledgement is provided within defined time standards, together with information on process, timelines, and confidentiality. Triage determines routing: safeguarding to specialised teams under survivor-centred protocols; fiduciary/procurement to the PIC and ECIC; environmental/social to E&S specialists; data-protection to the Data Protection Officer; and systemic issues to Internal Audit for thematic review.

4.5 Assessment and response. For each grievance, a proportionate assessment is conducted, including fact-finding, site visits where applicable, and review of records. Proposed responses—ranging from explanation and corrective action plans to restitution, specific performance, or escalation to sanctioning bodies—are reasoned, time-bound, and communicated to the complainant. Where consented, joint problem-solving or mediation may be used to reach agreement on remedies.

4.6 Safeguarding grievances (SEA/SH and child protection). Allegations of sexual exploitation, abuse, or harassment, or harm to children or vulnerable adults, are handled under survivor-centred protocols that prioritise safety, confidentiality, informed choice, and referral to appropriate services. Mandatory reporting obligations under domestic law are honoured. Access to records is strictly controlled, and

publication occurs only in anonymised, aggregate form, unless otherwise required by law and consistent with survivor consent.

4.7 Worker grievances. Contractors shall establish worker GRMs aligned with this Chapter, with protections against retaliation, translation services as needed, and clear escalation to the project-level GRM where employer responses are inadequate or conflicts arise. Worker GRM performance forms part of vendor performance assessments and may trigger contractual remedies.

4.8 Appeals and escalation. If a complainant disputes the proposed resolution or experiences delay beyond service standards, an appeal may be lodged to a higher tier within the GRM. Unresolved or systemic issues may be escalated to the Audit and Risk Committee or the Executive Board, and, where appropriate, referred to external authorities. The GRM does not impede access to courts, regulators, or national human rights institutions.

4.9 Timelines and service standards. The SLA prescribes service standards for acknowledgement, initial response, investigation duration, resolution, and appeal handling, differentiated by grievance type and severity. Exceptions for complex cases require reasoned extensions communicated to complainants. Performance against standards is tracked as KPIs and disclosed in quarterly dashboards.

4.10 Confidentiality, data protection, and publication. GRM records are processed under the Data Protection and Digital Trust Policy, with access limited to authorised personnel. Personally identifiable information is minimised and, where possible, separated from case summaries. Public reporting includes counts, categories, average resolution times, outcomes, and systemic corrective actions, with aggregation and redaction to preserve privacy and safety. Whistleblower identities are protected to the maximum extent lawful.

4.11 Remedies. Remedies may include acknowledgement and apology, correction of records, specific performance (e.g., remediation of environmental impacts), compensation where lawful and appropriate, modification of design or procedures, disciplinary action, contract variation or termination, and referral to sanctioning or investigative authorities. Remedy selection is reasoned, proportionate, and documented with evidence of completion.

4.12 Interface with procurement protests. Bidder protests and vendor disputes follow the procurement protest procedure embedded in the solicitation and contract and are logged within the GRM registry for transparency and systemic learning. Protest decisions are reasoned, recorded, and published with lawful redaction.

4.13 Learning and systemic improvement. Aggregated GRM analytics inform risk registers, audit plans, procurement specifications, design adjustments, and training curricula. Lessons-learned are presented periodically to relevant committees, including the ARC, PIC, PDC, and DPDTC, with tracked actions and publication of summaries.

4.14 Hosted Ownership considerations. Under Hosted Ownership, the GRM must clearly communicate title-holding arrangements and the respective responsibilities of GSIA/EUSL and the Member. Remedies must preserve ring-fencing and the reversion covenant. Where domestic institutional capacity is limited, capacity-building for local GRM counterparts is integrated into domestication benchmarks.

4.15 Records and retention. GRM case files, including submissions, communications, assessments, decisions, remedies, and closure documents, are retained in accordance with the records schedule and

legal holds. Integrity safeguards, including immutable logging and hash-anchoring of key artefacts, are applied to preserve evidentiary value for audits, evaluations, and dispute resolution.

4.16 Non-retaliation. Any actual or attempted retaliation against complainants, witnesses, or facilitators is a serious breach subject to sanctions under Document 11, vendor disqualification, and, where applicable, referral to authorities. Protective measures, including confidentiality, interim accommodations, and secure reporting channels, are implemented and monitored.

4.17 Interfaces. This Chapter interfaces with Document 03 (publication, incident handling), Document 05 (committees and secretariat records), Document 08 (MEL integration and verification), Document 10 (continuity during incidents), Document 11 (investigations and sanctions), and Document 12 (data protection). It does not derogate from ring-fencing, publication, or reversion obligations.

Chapter 5 — Fiduciary Risk Controls

5.1 Purpose and scope. This Chapter establishes the mandatory fiduciary risk-control architecture applicable to all GSIA engagements, including Flowhub Trio Plus operations under both the Standard Custodianship and Hosted Ownership variants. It governs GSIA SCE, GSIA Holding AB, GSIA AB, EUSL-designated special-purpose vehicles, Members and Hybrid RECs acting as competent authorities, and all vendors, fiduciaries, and financiers operating within ring-fenced perimeters. These controls are non-derogable save for reasoned, time-limited exceptions approved by the competent GSIA SCE oversight organ and recorded for publication with lawful redaction.

5.2 Control objectives. Fiduciary controls shall achieve the following objectives: (i) preserve the integrity and lawful use of funds and assets; (ii) ensure traceability from appropriation to outcome; (iii) deter, detect, and correct misstatement, fraud, or waste; (iv) enable timely, reliable reporting and audit; (v) maintain continuity under stress; and (vi) support domestication by progressively transferring control capability to the Member.

5.3 Minimum Control Set (MCS). Every project perimeter implements, documents, and tests the MCS, comprising at minimum:
(a) **Ring-fenced structures** for bank accounts, ledgers, records, and repositories;
(b) **Authority matrix** enforcing segregation of duties and four-eyes approvals with beneficiary countersignature thresholds;
(c) **Budgetary controls** linking commitments to approved funding lines and payment waterfall priorities;
(d) **Procurement integrity controls** including competitive methods, change-order thresholds, protest channels, and conflict screening;
(e) **Cash management** with daily position monitoring, bank reconciliations, and exception handling;
(f) **Asset controls** for physical and intangible property (registers, tags, periodic counts, impairment and write-off rules);
(g) **Financial reporting** on monthly and quarterly cycles with variance analysis and certification;
(h) **Audit trails** via immutable logs for key events and approvals;
(i) **Incident management** with classification, notification, containment, and cure periods; and
(j) **Publication controls** embedding transparency in the lifecycle.

5.4 Risk assessment and control tailoring. A fiduciary risk assessment is performed at inception and refreshed at least annually, classifying risks (inherent and residual) across domains including liquidity, FX, counterparty, political, legal, cyber, and operational risks. Controls may be strengthened above the

MCS in higher-risk contexts; weakening below the MCS is prohibited. Risk registers are maintained, linked to KRIs, and reviewed by the Audit and Risk Committee.

5.5 Cash, liquidity, and FX risk.
(a) **Liquidity buffers** are sized to meet near-term obligations under conservative assumptions and are held within the perimeter; use requires reasoned approval and is disclosed.
(b) **Payment cut-offs and batching** reduce timing risk; emergency rails are defined in continuity protocols.
(c) **FX exposure** is identified at contract and budget levels; where permitted and cost-effective, hedging instruments or natural hedges are used; FX gains/losses are disclosed through the ring-fenced statements.
(d) **Bank selection** follows prudential and AML/CFT due diligence; mandates embed dual signatories and limit bank liens to fees expressly agreed for the ring-fenced accounts.

5.6 Commitment and disbursement controls.
(a) **Commitment control** requires verified budget availability and alignment to procurement plans.
(b) **Milestone gating** links disbursements to documented acceptance and, where required, independent verification.
(c) **Advances** require appropriate security (e.g., guarantees) and recovery schedules tied to deliverables.
(d) **Holdbacks and retentions** are applied to manage performance risk and released against defect-liability criteria.

5.7 Counterparty and concentration risk.
(a) **Counterparty due diligence** is calibrated to risk (ownership, sanctions, solvency, capacity, integrity).
(b) **Concentration thresholds** are set for vendor, sector, and geographic exposure; breaches require reasoned approval and mitigation plans.
(c) **Step-in and replacement** clauses are mandatory to preserve continuity.

5.8 Journal, reconciliation, and close controls.
(a) **Journals** are supported by contemporaneous evidence with preparer and approver identity; manual journal entries are minimized and flagged for review.
(b) **Bank and sub-ledger reconciliations** are completed to a defined cadence, with aging of unreconciled items and escalation thresholds.
(c) **Period close** follows a documented checklist with certifications by GSIA AB finance and the Member's designated fiduciary.

5.9 Estimates, provisions, and impairments. Policies for estimates (e.g., accruals, provisions for doubtful accounts, warranty liabilities) are documented, conservative, and consistently applied. Significant judgments are recorded with rationale and approved at defined levels. Asset impairment tests are conducted at least annually or upon triggering events.

5.10 Information systems and digital controls.
(a) **IAM** enforces least-privilege; privileged access is just-in-time with dual-control and logging.
(b) **Configuration baselines** and change management are documented and approved; segregation between development, test, and production is enforced.
(c) **Logging and SIEM** collect, retain, and alert on events relevant to fiduciary control; integrity is ensured via append-only or hash-anchored logs.

(d) **Data governance** aligns with Document 12; financial data lineage is documented from source to report.

5.11 KRIs and KPI linkage. Fiduciary KRIs include reconciliation delays, exception rates, procurement variance patterns, single-source reliance, incident counts and severity, access anomaly rates, FX exposure levels, and late publication markers. KRIs are monitored against thresholds and linked to SLA KPIs and escalation rules.

5.12 Incident response and remediation. Incidents (fraud indicators, control failures, data integrity issues) trigger immediate containment, notification within SLA timelines, root-cause analysis, corrective action plans, and verification of closure by Internal Audit. Where material, publication is made in summary with lawful redaction.

5.13 Hosted Ownership safeguards. When legal title is held by GSIA Holding AB or an EUSL SPV:
(a) **Title and encumbrance registers** are maintained, updated, and periodically certified;
(b) **Negative pledge** and **no private distribution** covenants are embedded in all financing and counterparty instruments;
(c) **Reversion readiness** (clean title, lien releases, assignment/novation consents) is tracked as a standing control objective; and
(d) **Insurability** and loss-payee structures preserve Member benefit and ring-fenced restoration.

5.14 Documentation and publication. Policies, procedures, authority matrices, and risk registers are maintained in tamper-evident repositories; quarterly summaries of fiduciary control performance are published with lawful redactions. Any time-limited publication exception requires reasoned resolution and periodic review.

5.15 Interfaces. This Chapter interfaces with Document 03 (custody, SLAs, exit), Document 04 (leasing and domestication), Document 05 (internal audit and committee oversight), Document 10 (stress testing and continuity), Document 11 (investigations and sanctions), and Document 12 (digital trust). Nothing herein derogates from ring-fencing or reversion covenants.

Chapter 6 — Compliance Monitoring

6.1 Purpose and architecture. Compliance Monitoring verifies, on a continuing and independent basis, adherence to the ESG safeguards and fiduciary controls codified across Documents 03–06, detects deviations, and ensures timely correction without impairing continuity. It operates as a second-line function distinct from first-line management and third-line Internal Audit, reporting to the Audit and Risk Committee with administrative support from the Secretariat.

6.2 Scope and standards. Monitoring covers: (i) environmental and social management plans and performance; (ii) gender and inclusion safeguards and safeguarding protocols; (iii) anti-corruption, conflicts, and procurement integrity; (iv) fiduciary controls and KRIs; (v) data-protection and digital-trust obligations; (vi) publication and records duties; and (vii) domestication benchmarks and gates. Standards are defined in control libraries and mapped to test procedures.

6.3 Planning and cadence. An annual Compliance Monitoring Plan is approved by the Audit and Risk Committee, prioritising higher-risk perimeters and upcoming domestication gates. The plan defines continuous monitoring (automated controls and dashboards), periodic reviews (monthly/quarterly), and targeted thematic reviews triggered by incidents, KRIs, or committee requests. Deviations from the plan are permitted by reasoned memorandum addressing risk.

6.4 Methods and evidentiary discipline. Monitoring employs document and ledger reviews, data analytics, system log interrogation, site visits, interviews, re-performance, and sample-based testing. Evidence is preserved with chain-of-custody protocols and stored in tamper-evident repositories. Where technology permits, near-real-time exception dashboards are used to surface deviations in approvals, access, and procurement sequences.

6.5 Findings, classification, and timelines. Findings are classified by severity and impact on control objectives (e.g., Critical, High, Medium, Low). Each finding includes a clear statement of condition, criteria, cause, effect, and risk, with agreed corrective actions, responsible owners, and due dates. Critical and High findings trigger immediate management attention and reporting to the Audit and Risk Committee; persistent or systemic issues are flagged for Internal Audit follow-up.

6.6 Management response and verification. First-line management prepares written responses and corrective action plans within defined timelines. Compliance verifies implementation through evidence review and, where warranted, on-site checks. Closure requires objective evidence and, for Critical/High items, independent validation by Internal Audit.

6.7 Dashboards, reporting, and publication. Periodic compliance dashboards present status of findings, overdue actions, KRI trends, publication timeliness, procurement integrity markers, safeguarding incidents (anonymised), and domestication readiness indicators. Dashboards and narrative reports are submitted to the Audit and Risk Committee and summarised for public release with lawful redaction.

6.8 Escalation and sanctions interface. Failure to implement corrective actions within agreed timelines triggers escalation to the Executive Board and, where applicable, invocation of contractual remedies, budgetary conditions, or sanctions under Document 11. Repeated non-compliance may pause domestication gates or trigger step-in measures proportionate to risk.

6.9 Independence and resourcing. The Compliance function is staffed with competencies in E&S, safeguarding, procurement, finance, and digital trust, and is organisationally independent from operational delivery and from Internal Audit. Budget sufficiency and access rights are protected by resolution of the Executive Board. Staff are subject to conflict-of-interest and recusal rules and complete periodic training.

6.10 Technology and automation. Compliance leverages automated controls and monitoring tools to detect segregation-of-duties violations, approval anomalies, single-source patterns, late publications, access abuses, and unusual payment sequences. Rulesets are documented, tested, and version-controlled. Alerts are triaged, investigated, and closed with evidence, and tuning is performed to balance sensitivity and false positives.

6.11 Hosted Ownership monitoring. Additional tests verify title integrity, encumbrance status, lien-release progress, financing covenant compliance with no-distribution rules, and reversion readiness. Compliance coordinates with the Hosted Ownership Oversight Committee to ensure findings are addressed ahead of domestication gates.

6.12 Interfaces and learning. Compliance coordinates with: Internal Audit (assurance maps, reliance, and hand-offs); the Secretariat (publication and records); PIC and ECIC (procurement integrity and investigations); DPDTC (privacy and security controls); and PDC (domestication readiness). Lessons-learned inform template improvements, training, and control library updates.

6.13 Records and retention. Plans, workpapers, evidence, reports, dashboards, and closure documentation are retained in tamper-evident repositories per the records schedule and legal holds. Public summaries of compliance activity are published quarterly with lawful redaction.

6.14 Continuous improvement. The Compliance function performs annual self-assessments against its charter and best-practice frameworks and undergoes periodic independent reviews. Improvement plans, competency development, and technology roadmaps are approved by the Audit and Risk Committee and published in summary.

6.15 Non-retaliation and integrity. Individuals who raise concerns or cooperate with monitoring do so under non-retaliation protections. Allegations of retaliation are investigated promptly and may result in sanctions. Confidentiality is preserved consistent with due process and publication obligations.