NOVEMBER 4, 2025

# FLOWHUB TRIO PLUS GOVERNANCE AND OPERATING MANUAL

*CODIFYING GOVERNANCE-AS-A-SERVICE ARCHITECTURE, FIDUCIARY CUSTODY, AND DOMESTICATION PATHWAYS UNDER GSIA'S CONSTITUTIONAL MANDATE*

**CREATED BY**
EUSL AB
*Care to Change the World*

# Table of Contents

# Flowhub Trio Plus Governance and Operating Manual

## Chapter 1 — Governance-as-a-Service Architecture

**1.1 Purpose and scope.** This Manual operationalises the Flowhub Trio Plus construct within the GSIA institutional design approved in Documents 00–02. It defines the architecture, instruments, and oversight logic by which GSIA provides temporary, benchmarked governance-as-a-service to Members and their competent authorities, ensuring fiduciary integrity, verifiability, and a domestication pathway to public stewardship. The Manual binds GSIA Holding AB, GSIA AB, and GSIA SCE, and governs all Flowhub engagements with States, Regional Economic Communities (RECs), and Hybrid RECs admitted under Document 02.

**1.2 Constitutional placement and prevalence.** The Charter of GSIA SCE prevails over private instruments in all public-interest matters. This Manual is subordinate to the Charter and implements it. Where an inconsistency arises between (i) this Manual or any Service Level Agreement (SLA), Implementation Agreement, or Leasing Instrument, and (ii) the Charter, the Charter governs. GSIA Holding AB and GSIA AB shall ensure that all Flowhub contracts incorporate this prevalence clause and recognise the public-interest mandate of GSIA SCE.

**1.3 Separation of functions.** Separation of functions is mandatory and non-derogable:
(a) **GSIA SCE (Membership Body)** exercises mandate, policy direction, admissions, and oversight through its organs and voting rules as set by Documents 00–02. It approves the use of Flowhub where public-interest objectives, risk, or capacity criteria justify temporary custodianship.

(b) **GSIA Holding AB (Stewardship/IP)** safeguards intellectual property, standards, and certification marks of Flowhub, licenses their use to GSIA AB and approved operators, and protects the ring-fenced "no private distribution" doctrine applicable to the governance commission and risk buffers.

(c) **GSIA AB (Operations)** provides governance-as-a-service under SLA, operates project custody arrangements, maintains records and controls, and reports to GSIA SCE's oversight organs. Where appropriate, GSIA AB may appoint country or REC-level operators under back-to-back SLAs, preserving all controls and audit rights.

**1.4 The Flowhub "Trio Plus" model.** Flowhub comprises three primary service pillars and one enabling layer:
(a) **Governance (Pillar I)**: policy translation, institutional interface, decision-minute custody, publication controls, and adherence to Charter-mandated oversight.

(b) **Fiduciary (Pillar II)**: project custody, ring-fenced bank and ledger structures, procurement integrity, disbursement controls, and assurance.

(c) **Delivery (Pillar III)**: implementation orchestration, milestone gating, vendor and contract administration, and readiness for transfer.

(d) **Plus (Enabler)**: capacity building, digital trust and data protection, and risk/continuity functions that permit secure, scalable operations and domestication. The "Plus" layer is enabling only; it does not displace public authority, and it is designed to become redundant upon domestication.

**1.5 Lines of accountability.** Flowhub is accountable upward to GSIA SCE through the organs established in the Charter (Assembly, Executive Council/Board, and independent oversight functions), laterally to beneficiary public authorities through contractually defined joint approvals, and outward to stakeholders through publication duties. Decision rights are allocated as follows:

(i) GSIA SCE authorises Flowhub activation, sets domestication benchmarks, and approves exceptions to standard controls.

(ii) GSIA AB implements controls within the scope of the SLA, subject to four-eyes approvals and auditability.

(iii) Beneficiary authorities co-approve commitments and disbursements as defined in the authority matrix annexed to each SLA or Implementation Agreement.

(iv) Independent audit and ethics functions report to the oversight organ of GSIA SCE with unfettered access to records.

**1.6 Instruments and privity.** Governance-as-a-service is delivered through an integrated instrument set: (a) a Program Participation Agreement (PPA) between GSIA SCE and the Member defining mandate and coverage; (b) an SLA between GSIA AB and the Member's competent authority defining services and KPIs; (c) an Implementation Agreement governing delivery, milestones, vendor engagement, and publication; and, where Flowhub serves as temporary custodian, (d) a Leasing Instrument defining the dominium split between beneficial ownership and operational custody. All private-law instruments are made expressly subject to the Charter and to this Manual.

**1.7 Ring-fencing and records.** All Flowhub projects operate on a ring-fenced basis. Cash, assets, receivables, payables, and contingent items are segregated per project or per portfolio as agreed, with separate bank accounts, ledgers, and document repositories. Records include decisions, approvals, contracts, invoices, delivery and acceptance certificates, and performance data. Records are maintained in tamper-evident systems with immutable logs, time-stamps, and traceable version history. Retention schedules are adopted to preserve probative value and to support publication duties while respecting data-protection rules.

**1.8 Four-eyes, segregation of duties, and dual approvals.** No commitment or disbursement occurs without at least two independent approvals, one of which must be exercised by a signatory representing the beneficiary authority or its designated fiduciary, unless an emergency continuity protocol, duly recorded, is invoked in accordance with Chapter 6. Initiation, review, approval, and custody roles are separated. System access follows least-privilege and need-to-know principles, with duty rotation to reduce fraud risk.

**1.9 Publication and transparency.** Flowhub treats publication as a governance control. Unless restricted by law, security, or safeguarding obligations, Flowhub will publish, at minimum, approved SLAs (with sensitive elements redacted), KPIs and quarterly dashboards, procurement notices and awards, summary financial statements of ring-fenced accounts, conflict-of-interest disclosures, and rectification actions. Exceptions require a reasoned resolution recorded by GSIA SCE's oversight organ and are time-limited.

**1.10 Finance and governance commission.** Subscriptions are governed by Document 13. The Flowhub governance commission shall not exceed five percent (5%) of relevant project inflows as approved by GSIA SCE. The commission and the risk/capacity buffers are ring-fenced and may fund governance controls, assurance, capacity building, and domestication support only; they are not available for

private distribution. Residual balances are applied to Member benefit in accordance with GSIA SCE resolutions.

**1.11 Domestication benchmarks and readiness gates.** Flowhub is temporary. Each engagement incorporates domestication benchmarks, including institutional capacity, control environment maturity, data-protection conformance, and fiduciary performance. Benchmarks are tested at pre-defined gates. Upon meeting thresholds, custody and operational control are transferred to the competent public authority under the Exit and Transition Protocols (Chapter 6). Benchmarks and KPIs are embedded contractually in the SLA (Chapter 3) and in the Leasing Mechanism (Chapter 4).

**1.12 Conflict and precedence.** In any conflict between a Flowhub instrument and (i) national public law of the Member, (ii) the GSIA Charter, or (iii) this Manual, the order of application is: mandatory national public law; GSIA Charter; this Manual; specific Flowhub instrument. Where conflict would frustrate the public-interest mandate, the parties will adopt a reasoned amendment or a Host Country Agreement provision to cure the inconsistency, consistent with Document 07.

**1.13 Interfaces with forthcoming chapters.** KPIs and service standards are defined in Chapter 3. The leasing and domestication pathway is set out in Chapter 4. Data protection and digital trust are codified in Chapter 5. Exit and transition are governed by Chapter 6. Nothing in this Chapter shall be construed to limit the specificity of those provisions.

## Chapter 2 — Project Custody and Fiduciary Controls

**2.1 Custody doctrine.** Project custody under Flowhub is a temporary, benchmarked custodianship exercised by GSIA AB (or an approved operator) solely to protect public assets, ensure value for money, and accelerate domestication. Custody does not confer ultimate ownership. It is exercised within a ring-fenced fiduciary perimeter and ends upon readiness certification.

**2.2 Beneficial ownership.** Beneficial ownership of project assets, rights, and proceeds resides with the Member's competent public authority at all times. Where law requires, assets may be held by a special-purpose vehicle (SPV) or in trust/escrow in favour of the Member. Title instruments, asset registers, and security filings shall recite the beneficial-ownership clause and the temporary nature of Flowhub custody.

**2.3 Project vehicles and accounts.** Each project operates through one of the following, as specified in the Implementation Agreement:

(a) a **ring-fenced account structure** under GSIA AB, with separate bank accounts, ledgers, and document repositories; or

(b) a **special-purpose vehicle** incorporated under appropriate law (e.g., AB/SCE or equivalent), wholly ring-fenced by statute and contract, with GSIA AB as custodian and the competent authority as beneficiary; or

(c) a **trust/escrow arrangement** with a licensed fiduciary, appointing GSIA AB as operator and the competent authority as beneficiary.

Whichever form is used, the minimum control set in this Chapter applies.

**2.4 Segregation of duties and authority matrix.** An authority matrix, annexed to each SLA, defines initiation, review, approval, payment, and reconciliation roles. At minimum, (i) initiators cannot approve; (ii) approvers cannot reconcile; (iii) system administrators cannot initiate or approve

transactions; and (iv) no single person may complete a commitment or payment end-to-end. Threshold-based escalations require higher-level approvals and, at defined levels, the countersignature of the beneficiary authority.

**2.5 Dual approvals and the four-eyes rule.** All commitments and payments require dual approvals. One approver must be independent of the initiating unit; for payments above threshold, one approver must be the beneficiary authority or its designated fiduciary. Electronic approvals must rely on strong identity assurance and tamper-evident audit trails. Emergency derogations are permitted only under continuity protocols and must be regularised within defined time limits.

**2.6 Cash management and payment waterfall.** Cash inflows are received into ring-fenced bank accounts. A payment waterfall, set out in the Implementation Agreement, allocates funds by priority: (i) statutory and mandatory charges; (ii) contracted deliverables and verified milestones; (iii) governance commission and risk/capacity buffers (≤5%) in accordance with Clause 1.10; and (iv) reserves and contingencies. Surpluses are retained within the ring-fenced perimeter or applied to Member benefit by reasoned resolution. Inter-project transfers are prohibited unless expressly authorised and documented.

**2.7 Procurement integrity and commitments.** All procurement follows an approved Procurement Plan, with transparent solicitation, objective evaluation, and documented award decisions. Commitments may not be entered into without budget availability and approved funding lines. Variations and change orders are subject to the same controls as initial awards. Conflicts of interest are disclosed ex ante; recusal is mandatory for conflicted persons. Blackout periods and communication protocols are established to preserve integrity.

**2.8 Ledgers, records, and audit trails.** Each project maintains a discrete chart of accounts, journals, and sub-ledgers for commitments, obligations, accruals, and disbursements. All records are time-stamped, immutable, and linked to underlying evidence (contracts, invoices, delivery notes, inspection reports, acceptance certificates). System logs capture identity, time, action, and object changed. Periodic reconciliations are documented and certified by both GSIA AB and the beneficiary authority.

**2.9 Reporting and publication.** Minimum reporting includes monthly cash and commitment reports, quarterly financial statements of ring-fenced accounts, quarterly KPI dashboards, and semi-annual procurement summaries. Public versions are published with necessary redactions. Management letters, internal-audit findings, and remediation plans are reported to the GSIA SCE oversight organ and, where applicable, published in summary form. Exceptions to publication require reasoned, time-limited resolutions.

**2.10 Governance commission, buffers, and no-distribution rule.** The governance commission and risk/capacity buffers are accounted for in separate cost centres within the project perimeter. Expenditure from these lines is limited to governance services, independent assurance, risk mitigation, capacity building, and domestication support. No dividends or private distributions are permitted. Any residual balances at project close are applied as directed by GSIA SCE for Member benefit.

**2.11 Bank mandates and financial institutions.** Bank mandates require dual signatories in accordance with the authority matrix and include the beneficiary authority's mandate at defined thresholds. Banks and fiduciaries are selected against due-diligence criteria covering prudential soundness, AML/CFT controls, sanctions compliance, data-protection posture, and digital-trust capabilities. Account opening and changes follow documented approvals and KYC updates.

**2.12 Verification and acceptance.** Disbursements against deliverables require documented verification and acceptance by the competent technical authority. Where independent verification is mandated, release of funds is contingent upon a verification report meeting pre-agreed standards. Partial acceptances and holdbacks are permitted where technically justified and recorded.

**2.13 Breach, suspension, and remedies.** Material breaches of fiduciary controls trigger suspension of commitments and payments within the affected perimeter, pending corrective action. Remedies include claw-back, re-procurement, replacement of vendors, personnel removal, and referral to investigation under the Ethics Code (Document 11). Sanctions are proportionate, reasoned, and recorded. Members retain all rights available under applicable public law.

**2.14 Interfaces with risk, continuity, and data protection.** Fiduciary controls are integrated with (i) enterprise and programmatic risk management (Document 17), including key risk indicators and escalation triggers; (ii) continuity of operations and contingency planning (Document 10), including emergency payment protocols and cold-site arrangements; and (iii) data-protection and digital-trust safeguards (Chapter 5 and Document 12), including data minimisation, access controls, encryption, and cross-border transfer rules. These interfaces are mandatory and will be cross-referenced in SLAs.

**2.15 Readiness testing and transfer.** Custody ends upon certification that domestication benchmarks in the SLA and Leasing Instrument have been met. Certification is issued by GSIA SCE's designated organ upon review of fiduciary performance, control maturity, staffing and systems readiness, and legal sufficiency for transfer. The mechanics of exit, including assignment of contracts, transfer of accounts and records, and continuity of obligations, are governed by Chapter 6.

## Chapter 3 — Service Level Agreements and KPIs

**3.1 Nature and hierarchy of the SLA.** The Service Level Agreement constitutes the binding instrument by which GSIA AB delivers governance-as-a-service to a Member's competent authority under the mandate conferred by the GSIA SCE through the Program Participation Agreement. The SLA is an implementing contract that operationalises the Charter and this Manual. In case of inconsistency, mandatory national public law prevails, followed by the GSIA Charter, this Manual, and the SLA, in that order. The SLA shall incorporate by reference the fiduciary controls (Chapter 2), the leasing and domestication mechanics (Chapter 4), the data-protection and digital-trust annexes (Chapter 5), and the exit and transition protocols (Chapter 6).

**3.2 Parties and privity.** The SLA is executed between GSIA AB and the Member's competent public authority, with GSIA SCE cited as mandate-grantor and beneficiary of audit and oversight rights. Where a delegated operator is engaged, a back-to-back SLA is concluded on identical or more stringent terms, preserving audit, inspection, publication, and step-in rights for GSIA SCE and the Member.

**3.3 Scope of services.** The SLA delineates services under the Flowhub Trio Plus architecture: (a) **Governance services** including policy translation, decision-minute custody, publication management, organ liaison, and compliance with Charter-mandated oversight.

(b) **Fiduciary services** including custody of ring-fenced accounts, dual approvals, procurement integrity, reporting, and assurance coordination.

(c) **Delivery orchestration** including milestone gating, vendor/contract administration, verification coordination, and readiness preparation.

(d) **Enabling "Plus" services** including capacity-building for domestication, digital-trust enablement, and risk/continuity integration. The SLA is precise and exhaustive; services not listed are excluded unless added by reasoned amendment.

**3.4 Authority matrix and segregation of duties.** An authority matrix is annexed to the SLA, specifying initiation, review, approval, payment, reconciliation, and publication roles. The matrix codifies four-eyes approvals, beneficiary countersignature thresholds, escalation levels, and emergency derogation procedures. No person may complete a commitment or payment end-to-end. System administration is segregated from transactional roles.

**3.5 Service levels and time standards.** The SLA establishes time-bound service standards measured from receipt of complete documentation:
(i) procurement cycle stages (notice, evaluation, award, contract execution);
(ii) payment processing after verified acceptance;
(iii) publication of required disclosures;
(iv) monthly, quarterly, and ad hoc reporting issuance;
(v) rectification timelines for audit findings and incidents;
(vi) onboarding and domestication milestones. Standards are expressed in calendar days with defined business-day calendars and cut-off times. Extensions require a reasoned notice and do not waive underlying obligations.

**3.6 KPI framework.** The SLA contains a KPI schedule with baselines, targets, measurement methodology, evidence sources, and verification rights. KPIs shall include, at minimum:
(a) **Fiduciary integrity KPIs**: percentage of transactions with dual approvals; reconciliation timeliness; exception rates; on-time bank reconciliations; compliance with ring-fencing (zero unauthorised inter-project transfers).
(b) **Procurement integrity KPIs**: competitive processes share; protest/incidence rates; time to award; percentage of awards published; conflict-of-interest disclosure compliance.
(c) **Delivery performance KPIs**: milestone achievement on schedule; independent verification pass rates; change-order frequency and value; vendor performance index.
(d) **Governance and transparency KPIs**: publication timeliness; completeness of quarterly dashboards; time to respond to oversight inquiries; implementation of audit recommendations.
(e) **Domestication KPIs**: staff competency uplift against curriculum; successful shadow-to-lead transitions in defined functions; systems handover readiness; legal instrument localisation progress.
(f) **Data protection KPIs** (interfacing with Chapter 5): access-control conformance; audit-log completeness; incident mean time to detect and to contain; data-minimisation adherence for MEL datasets.

**3.7 Performance tiers and remedies.** The SLA defines performance tiers:
— **Tier A (On-target or better):** no remedy; eligibility for accelerated domestication testing and reduced oversight frequency after reasoned resolution.
— **Tier B (Within tolerance):** corrective action plan with time-bound milestones; intensified monitoring.
— **Tier C (Below tolerance):** formal remediation, suspension of non-essential commitments within the affected perimeter, and potential step-in by GSIA SCE under oversight authority. Persistent Tier C triggers sanctions pursuant to Document 11 and may delay domestication gates.

**3.8 Verification and assurance.** KPI attainment is evidenced through primary records, immutable logs, and independent verification where applicable. The SLA grants GSIA SCE oversight organs, internal

audit, and external auditors unfettered access to records within legal constraints, with reasonable notice and secure handling protocols. Where KPIs rely on third-party attestations, the SLA requires independence, competence, and documented methodology.

**3.9 Publication duties.** The SLA codifies publication of KPI dashboards, procurement summaries, ring-fenced financial statements, and conflict-of-interest registers, subject to lawful redaction. Non-publication requires a reasoned, time-limited exception approved by the GSIA SCE oversight organ and recorded.

**3.10 Change control.** The SLA includes a structured change-control procedure for scope, KPIs, service levels, and authority matrix adjustments. Changes must maintain or improve control strength, preserve ring-fencing, and be justified by capacity shifts, legal requirements, or domestication achievements. Material changes require approval by the GSIA SCE oversight organ and the Member's competent authority.

**3.11 Fees and the governance commission.** Fees are defined in the SLA in accordance with Document 13 and clause 1.10 herein. The Flowhub commission and buffers are capped at five percent (5%) and ring-fenced for governance controls, assurance, capacity building, and domestication support. The SLA prohibits private distribution and prescribes disclosure of commission utilisation.

**3.12 Incidents, cure periods, and escalation.** The SLA establishes incident classes (fiduciary, procurement, delivery, data-protection) with notification timelines, immediate containment measures, root-cause analysis, and cure periods proportionate to severity. Escalation progresses from operational leads to the GSIA SCE oversight organ and, where warranted, to the Member's designated high authority. Emergency derogations used to preserve continuity must be documented and regularised within defined limits.

**3.13 Interfaces and annexes.** Mandatory annexes include: the authority matrix; KPI schedule; procurement plan and integrity safeguards; reporting templates; publication schedule; data-protection addendum; continuity and emergency payment protocol; domestication pathway plan; and exit checklists. Cross-references are binding and incorporated as if set forth in full.

**3.14 Duration and renewal.** SLAs are issued for defined terms aligned to project cycles and domestication gates. Renewal is contingent on KPI attainment, audit opinions, and domestication progress. Sunset clauses apply to functions rendered redundant by domestication, with orderly handover as per Chapter 6.

## Chapter 4 — Leasing Mechanism and Domestication Pathway

**4.1 Nature and purpose.** The Leasing Mechanism is a temporary, benchmarked arrangement by which GSIA AB, as custodian, exercises operational control over defined project assets, contracts, and systems for the sole purpose of safeguarding public value and accelerating readiness of the Member's competent authority to assume full stewardship. The mechanism separates beneficial ownership (which remains with the Member) from temporary operational custody (exercised by GSIA AB) under strict fiduciary controls. It terminates upon domestication.

**4.2 Instrument structure.** The Leasing Instrument is a stand-alone contract, cross-referenced in the PPA and SLA, that:
(i) identifies the asset and contract perimeter subject to custody;
(ii) affirms beneficial ownership by the Member and the temporary character of custody;

(iii) incorporates ring-fencing, dual approvals, segregation of duties, and publication obligations;
(iv) sets domestication benchmarks and time-bound readiness gates;
(v) prescribes transfer mechanics, including assignment and novation of contracts, handover of accounts and records, and continuity of obligations; and
(vi) defines remedies, cure and suspension rights, and dispute-resolution venues consistent with Document 04 and Document 11.

**4.3 Asset perimeter and registers.** Assets may include cash, receivables, inventories, equipment, digital systems, licenses, data sets, and contractual rights. A verified asset register is established at inception, with valuation bases, encumbrances, and location. The register is updated for acquisitions, disposals, impairments, and transfers. Title documents and filings recite the beneficial-ownership clause and the custodial nature of GSIA AB's control.

**4.4 Operational control and limits.** GSIA AB exercises day-to-day operational control strictly within the perimeter and purposes stated. It may not pledge, encumber, or dispose of assets except as authorised in the Procurement Plan or Implementation Agreement. Any security interests granted to financiers are structured to preserve the Member's beneficial ownership and the ring-fenced character of the assets.

**4.5 Financial perimeter and covenanting.** Ring-fenced accounts and ledgers are mandatory. Covenants restrict inter-project transfers, unrelated expenditures, and deviations from the payment waterfall. Governance commission and buffers remain within the project perimeter and are subject to the no-distribution rule. Covenant breaches trigger suspension and corrective measures as per Section 4.11.

**4.6 Domestication pathway.** The Leasing Instrument embeds a domestication plan comprising staged benchmarks:
(a) **Functional shadowing:** public-authority staff are embedded to shadow Flowhub counterparts across fiduciary, procurement, delivery, and publication functions with defined competency objectives.
(b) **Dual-key operations:** approvals are exercised jointly, with progressive increases in thresholds under the Member's signature as competencies are certified.
(c) **Lead-role transition:** designated functions transition to public-authority lead with Flowhub in support, contingent on KPI attainment and control maturity.
(d) **System handover:** identity and access management, configuration, and administrative rights are transferred under dual-custody protocols; logs and records are exported and re-ingested under integrity checks.
(e) **Legal localisation:** standard operating procedures, templates, and instruments are localised to domestic legal requirements without diluting controls.

**4.7 Readiness gates and certification.** Progress is assessed at pre-defined gates, each tied to KPIs and control-maturity criteria. Certification of readiness for each gate is issued by the GSIA SCE oversight organ on the basis of documented evidence, internal-audit assurance, and, where applicable, independent validation under Document 09. Gate outcomes are recorded with reasons, and corrective actions are agreed when thresholds are not met.

**4.8 Transfer mechanics.** Upon final readiness certification:
(i) project bank mandates are amended to remove Flowhub custodians and appoint the public authority;
(ii) contracts are assigned or novated to the public authority, with vendor notices and continuity

undertakings;
(iii) physical and digital assets are transferred with acceptance certificates;
(iv) records, logs, and evidence repositories are delivered in agreed formats with integrity attestations; and
(v) warranties, claims, and contingent obligations are documented with responsibility matrices for post-transfer management.

**4.9 Publication and public notice.** The domestication event is published, including a summary of performance against benchmarks, the transfer date, and the identity of the assuming authority. Sensitive details may be redacted consistent with law and safeguarding obligations. Publication is a condition subsequent to transfer.

**4.10 Capacity-building completion and residual support.** The domestication plan includes a time-limited residual support period during which GSIA AB provides advisory services under a diminishing scope. Residual support is funded from the ring-fenced capacity-building buffer or, where exhausted, by a separate appropriated line agreed by the Member. Residual support does not re-establish custody.

**4.11 Breach, cure, and suspension within leasing.** Material breaches of fiduciary covenants or domestication obligations by any party trigger a notice with cure periods proportionate to severity. Absent cure, GSIA AB may suspend operational control transitions or, where the breach is by Flowhub, the Member may suspend or terminate the Leasing Instrument with step-in or replacement remedies. All actions are recorded by reasoned resolutions and reported to GSIA SCE oversight organs.

**4.12 Early termination and reversion.** Early termination may occur for convenience by mutual agreement, force majeure, legal impossibility, or persistent material breach. Termination results in immediate reversion of operational control to the Member, subject to continuity measures to avoid service disruption. The parties execute a termination protocol mirroring Section 4.8 to safeguard records, assets, and obligations.

**4.13 Interface with risk, continuity, and data protection.** The leasing arrangement integrates with the enterprise risk framework (Document 17), the financial stress-testing and continuity manual (Document 10), and the data-protection and digital-trust policy (Chapter 5 and Document 12). Emergency derogations to approval thresholds during continuity events are permitted only under documented protocols, are time-limited, and are subject to ex post audit and publication.

**4.14 No creation of private rights beyond mandate.** The Leasing Instrument creates no proprietary rights in GSIA AB or any private party beyond temporary operational custody. Licenses of intellectual property, software, and methods remain with GSIA Holding AB and are granted on a non-exclusive, revocable, non-transferable basis solely for public-interest performance within the project perimeter.

**4.15 Sunset and survivals.** Upon domestication or termination, custody sunsets. The following survive for the statute of limitations or agreed period: audit and access rights; warranties and indemnities; confidentiality; data-protection obligations; non-solicitation of key staff for a defined period where necessary to protect continuity; and dispute-resolution clauses.

## Chapter 5 — Data Protection and Digital Trust Integration

**5.1 Purpose and legal basis.** This Chapter codifies the data-protection and digital-trust requirements that govern all Flowhub operations. It defines the roles and responsibilities of GSIA SCE, GSIA Holding

AB, GSIA AB, Members, and their vendors and processors; prescribes identity, access, logging, and encryption controls; and sets domestication benchmarks for transfer of digital-trust functions to competent public authorities. Processing must have a lawful basis under applicable public law and data-protection statutes, be necessary and proportionate to the public-interest mandate, and be documented in a Data Processing Agreement (DPA) consistent with Document 07.

**5.2 Roles, accountability, and instructions.** The Member's competent public authority remains data controller for personal data processed within the Flowhub perimeter, unless a different allocation is mandated by law and recorded in the DPA. GSIA AB acts as data processor, and where it determines means of processing strictly for security, logging, or integrity purposes mandated by this Manual, it does so under the controller's instructions and accountability framework. Sub-processors engaged by GSIA AB operate only under written authorisation and flow-down obligations. GSIA SCE retains oversight rights but does not process data except for supervisory purposes delineated in the Charter and this Manual.

**5.3 Data categories and minimisation.** Data processed under Flowhub are limited to categories necessary for governance, fiduciary control, delivery orchestration, MEL, and publication. Categories include: (i) personal data of staff and vendors; (ii) sensitive personal data where legally required for safeguarding or workforce administration and subject to heightened controls; (iii) financial and procurement records; (iv) technical and delivery documentation; and (v) MEL datasets. Data minimisation applies to collection, retention, access, and publication. Where public reporting is required, aggregation, anonymisation, or pseudonymisation techniques shall be applied to meet transparency duties without disclosing unnecessary personal data.

**5.4 Privacy by design and impact assessments.** All systems, processes, and changes are designed to meet privacy principles by default. Data Protection Impact Assessments (DPIAs) are performed for high-risk processing, including biometric, geolocation, large-scale monitoring, or cross-border transfers of sensitive categories. DPIAs are reviewed by the Member's designated privacy authority and made available to GSIA SCE's oversight organ upon request, with lawful redactions.

**5.5 Identity and access management.** Access follows least-privilege and need-to-know principles, with strict segregation of administrative and transactional roles. Multi-factor authentication, conditional access, and just-in-time privileged elevation are mandatory for all administrative functions. Role designs mirror the segregation of duties in Chapters 1–2. Periodic access recertification is performed jointly by GSIA AB and the Member's competent authority and recorded.

**5.6 Logging, audit trails, and immutability.** Systems shall maintain immutable, time-stamped logs of access, configuration, data changes, approvals, and transactions sufficient to reconstruct decisions and actions. Logs are retained consistent with evidentiary and statutory requirements, protected from tampering, and accessible for audit under defined procedures. Chain-of-custody for extracted logs and records is documented and independently verifiable.

**5.7 Encryption and key management.** Data in transit and at rest are encrypted to standards appropriate to the sensitivity of the data and the legal environment. Key management is segregated from application administration and follows dual-control principles. Where hardware security modules or managed key vaults are used, custody and access policies are documented, and keys are rotated and retired under a defined schedule. Escrow of decryption keys for emergency access is permitted under continuity protocols with dual-custody.

**5.8 Cross-border transfers, localisation, and sovereignty.** Cross-border transfers of personal or sensitive operational data occur only where permitted by applicable law and under implemented safeguards, including adequacy determinations, standard contractual clauses, or equivalent mechanisms. Where localisation or sovereignty provisions require in-country storage and processing, Flowhub deploys in-region infrastructure and ensures that support operations do not compromise localisation. Host Country Agreement provisions (Document 07) may be invoked to clarify jurisdiction and lawful bases where necessary.

**5.9 Vendor and processor governance.** All vendors and processors with access to data or systems within the Flowhub perimeter are bound by a DPA annexed to the Implementation Agreement or to the procurement contract. Obligations include purpose limitation, confidentiality, security measures, sub-processor disclosure and approval, incident notification, cooperation with audits, and secure return or deletion at contract end. A public or Member-accessible sub-processor register is maintained and updated prior to engagement or material changes.

**5.10 Incident classification, notification, and response.** Incidents are classified at least as: (i) data-protection incidents; (ii) security breaches without confirmed personal-data impact; and (iii) availability or integrity degradations affecting fiduciary or delivery functions. The SLA prescribes detection, containment, notification, and remediation timelines, including regulatory and data-subject notifications where required by law. Root-cause analysis and corrective actions are documented and tracked as KPIs (Chapter 3) and reported under publication rules, with lawful redaction.

**5.11 Publication with privacy safeguards.** Publication duties in Chapters 1–3 are fulfilled using privacy-preserving techniques. Public dashboards and reports shall avoid direct identifiers unless required by law and shall apply aggregation thresholds to prevent re-identification. Where de-identification risks remain material, the GSIA SCE oversight organ may authorise narrow, time-limited exceptions to publication through a reasoned resolution.

**5.12 Digital-trust anchors.** Decision minutes, approvals, and milestone attestations are signed using verifiable digital signatures under a recognised trust framework. Time-stamping, hash-chaining, or equivalent append-only evidentiary measures are applied to critical records to support verifiability and non-repudiation. Configuration baselines and integrity checks are recorded to permit independent confirmation of system state at relevant times.

**5.13 Data-subject and stakeholder rights.** Where applicable law grants data-subject rights (access, rectification, erasure, restriction, portability, or objection), the controller (Member) defines procedures and service levels, and GSIA AB implements them as processor, including identity verification and logging. Legitimate restrictions may apply to protect investigations, safeguards, or legal obligations, and are recorded with reasons.

**5.14 Retention and deletion.** Retention schedules are defined per data category, balancing legal obligations, evidentiary needs, and minimisation. Upon domestication or termination, data are transferred to the competent public authority with integrity attestations. Residual copies are securely deleted or irreversibly anonymised, save for records lawfully retained for audit, dispute resolution, or statutory compliance, as specified in survivals (Section 6.8).

**5.15 Interfaces and domestication benchmarks.** This Chapter interfaces with Document 12 (Data Protection and Digital Trust Policy) for enterprise-level standards; with Document 08 (Unified MEL Framework) for indicators, baselines, and verification data governance; and with Document 10 (Financial Stress Testing and Continuity) for availability and resilience controls. Domestication

benchmarks include demonstrated capacity to administer identity and access, manage keys, maintain SIEM and audit-log operations, execute DPIAs, process data-subject requests, and operate publication safeguards. Readiness is certified at domestication gates pursuant to Chapter 4.

## Chapter 6 — Exit and Transition Protocols

**6.1 Purpose and principle.** Exit and transition operationalise the temporary character of Flowhub, ensuring orderly transfer of custody and operational control to the Member's competent authority once domestication benchmarks have been met, while preserving continuity of service, integrity of records, and enforceability of obligations. Exit shall not impair public value or legal rights and is effected through reasoned, documented procedures.

**6.2 Preconditions and certification.** Transition requires formal readiness certification under Chapter 4. Certification is issued by the GSIA SCE oversight organ on the basis of KPI attainment, control-maturity evidence, legal localisation, and demonstrated capacity of the receiving authority to administer fiduciary, delivery, and digital-trust functions. Any conditions precedent are stated with timelines and assigned responsibilities.

**6.3 Transition plan and governance.** A project-specific Transition Plan is established no later than the penultimate domestication gate. It identifies scope, timelines, responsibilities, dependency maps, risk controls, communications, and acceptance criteria. A joint Transition Steering Group comprising GSIA AB and the Member's authority supervises execution, records decisions, and resolves issues within defined escalation paths to the GSIA SCE oversight organ where required.

**6.4 Transfer packs and deliverables.** Transfer consists of structured deliverables, including: (i) updated asset registers and title instruments; (ii) financial statements of ring-fenced accounts, open commitments, contingent liabilities, and bank mandate change instructions; (iii) contract assignment or novation instruments with vendor notices and confirmations; (iv) system configuration baselines, access inventories, credential handover protocols, and key-management transition records; (v) complete records and immutable logs with integrity attestations; and (vi) current policies, procedures, and standard templates localised to domestic law. Acceptance is evidenced by countersigned certificates listing exceptions and remedies.

**6.5 Operational switch-over.** Switch-over follows a controlled sequence: (a) dual-running period with shadow/lead operations and live validations; (b) cut-over window during which credentials, mandates, and routing are switched; and (c) stabilisation period with heightened monitoring and incident response readiness. Emergency back-out criteria are pre-defined, strictly time-limited, and may be invoked only to protect continuity of essential services, with immediate documentation and oversight notification.

**6.6 Continuity safeguards.** Continuity measures include emergency payment protocols, escrow of critical credentials and keys under dual-custody, escrow of source or configuration artefacts where necessary to operate systems, fall-back SLAs with essential vendors, and cold-site or alternative processing arrangements consistent with Document 10. Derogations from normal approval thresholds to maintain continuity are permitted solely under documented continuity protocols and are regularised within defined time limits.

**6.7 Publication and public notice.** The domestication and transition event is publicly noticed as required by Chapter 4, including the transfer date, scope, and the assuming authority. Summary performance against benchmarks and outstanding conditions subsequent are disclosed with lawful

redaction. Publication occurs within the timeline set in the Transition Plan and is a condition subsequent to completion.

**6.8 Survivals and closures.** Upon completion, custody sunsets. The following obligations survive for the period specified by law or contract: audit and access to transferred records; warranties, indemnities, and vendor back-to-back guarantees; confidentiality and data-protection duties; cooperation with investigations and disputes; and retention of essential records by GSIA AB solely for statutory or audit purposes. Ring-fenced accounts, buffers, and residual funds are reconciled, audited, and either transferred or applied to Member benefit by reasoned resolution of GSIA SCE, with publication of the closure statement.

**6.9 Post-transfer support.** A time-limited residual support phase may be agreed for advisory, hypercare, or knowledge transfer. Residual support is funded per Chapter 4 and does not re-establish custody or alter the allocation of responsibilities. Support KPIs and exit criteria are defined and monitored.

**6.10 Disputes and rectification post-transfer.** Disputes arising from transfer mechanics, latent defects, or post-transfer performance are handled under the dispute-resolution provisions of the SLA and Leasing Instrument, read with Document 04 and Document 11. Rectification plans shall prioritise continuity and public value, be time-bound, and be reported to the GSIA SCE oversight organ. Where defects are attributable to vendors, step-in and warranty claims are pursued in the name of the Member or GSIA AB as appropriate.

**6.11 Records of decision and lessons-learned.** All material transition decisions, exceptions, and outcomes are minuted and archived. A lessons-learned report is produced within a defined period after completion, addressing performance against benchmarks, incident handling, vendor performance, and recommendations for future transitions. Public release follows the publication rules of Chapters 1–3.

**6.12 Interfaces.** This Chapter interfaces with Chapter 4 for domestication gates, with Chapter 5 for digital-trust handover, with Document 10 for continuity and contingency arrangements, with Document 08 for MEL closure and handover of indicator registries, and with Document 12 for enduring data-protection obligations.