# Terra Vita Hub

## Procurement-Safe Minimum Evidence Request

For ministries, sovereign programmes, MDBs/DFIs, procurement, vendor risk, IT/security and auditors.

### How to use this template

**Copy this request into your standard vendor-risk, IT-security, procurement or RFP questionnaire, or attach it as an annex to contract review. Formal approval should not proceed until the evidence below has been reviewed and validated by the relevant institutional teams.**

### 1. Governance and reviewer controls

- Reviewer role model and identity-preservation logic.
- Escalation pathways and override visibility.
- Decision-chain attribution: how reviewer actions are recorded and linked.
- Audit-event samples with timestamps, reviewer identity and evidence linkage.
- Evidence lineage demonstration: versioning, attribution and export posture.

### 2. Security, reliability and operational assurance

- Encryption posture at rest and in transit.
- Key management model.
- Tenancy model: single-tenant, sovereign or managed.
- Uptime bands and incident-response posture.
- RPO/RTO expectations and disaster-recovery model.
- Access-control model: roles, permissions and enforcement logic.

### 3. Data lifecycle and residency

- Data residency statement: jurisdiction, storage location and residency guarantees.
- Data retention and deletion logic.
- Evidence versioning and immutability posture.
- Export posture: formats, completeness and institution-controlled access.

### 4. Integration and interoperability controls

- Integration governance: approval, monitoring and change-control.
- API boundaries and data-ingestion controls.
- Spatial/MRV evidence handling: ingestion, validation and linkage.
- Programme-specific integration configuration, where applicable.

## 5. Programme-specific configuration

- Reviewer groups and assignment logic.
- Escalation configuration.
- Evidence classes used.
- Export and reporting configuration.
- Programme-specific constraints or custom governance rules.

## 6. Contractual commitments

- SLA: availability, response times and support model.
- Support and incident-response commitments.
- Data export and termination guarantees.
- Deployment-specific obligations such as residency, segregation or audit access.

## 7. Additional evidence, if applicable

- Independent auditability posture.
- Reviewer performance and consistency metrics: RPI/RCS.
- Bias and divergence detection posture: BDD.
- Programme calibration logic: PCL.
- Institutional oversight dashboard configuration: IOD.

## Institutional position

**This request reflects the minimum evidence required for institutional reliance. Public governance narrative is not a substitute for protected, verifiable, deployment-specific artefacts. Formal approval should not proceed until the evidence above has been reviewed and validated by procurement, IT/security, fiduciary teams and programme oversight.**