AVEUM

ECOSYSTEM GOVERNANCE & SUCCESSION BLUEPRINT

Pre-Operational Guide for the AVEUM Genomic Testnet Vault Ecosystem

PURPOSE
A practical governance and succession reference for institutions, family offices, fund managers, trustees and MPC operators preparing to enter the AVEUM vault ecosystem.

DESIGNED FOR
Corporate fund managers
Family offices
MPC / custody operators
Trustees and estate administrators

TECHNOLOGY AT A GLANCE

AVEUM is designed as a vault security and governance layer that can sit alongside institutional MPC custody. The model binds vault authorization to a biological identity-derived GIS, while smart-contract rules govern transfer paths, lock conditions and succession events.

THE GOVERNANCE MODEL

- Main Vault GIS provides master oversight and the only horizontal transfer authority.
- Each distinct GIS identity maps to one dedicated source wallet.
- Named-person sub-vaults require an individual genomic identity and operate within defined vertical transfer boundaries.
- Succession and inactivity rules are encoded into the deployed contract configuration.

EXECUTIVE SUMMARY

Before deployment, the critical task is not simply funding a wallet. It is confirming who controls the family or institutional structure, which identities are mapped to which vaults, how transfers are constrained, what happens during lock mode, and how the estate is expected to operate if a keepalive signature is not received.

Important: This guide is pre-operational. It should be reviewed by the appropriate legal, compliance, security and estate-planning professionals before any production deployment.

1. VAULT HIERARCHY & IDENTITY MAPPING

The AVEUM structure separates master oversight from individual identity-bound sub-vaults. The objective is to make authority, ownership and routing explicit before assets are introduced.

MAIN VAULT Master GIS Control & oversight	**SUB-VAULT A** Named person / role Individual GIS + source wallet	**SUB-VAULT B** Named person / role Individual GIS + source wallet
UNASSIGNED / MAIN-GIS Remains under Main Vault GIS control	**UNDER-18 ESCROW MODE** Held under Main Vault GIS until contract-defined transition	**OTHER CONFIGURED SUB-VAULTS** Up to the configured ecosystem limit

1:1 MAPPING RULE

Every distinct GIS identity maps to exactly one dedicated Source Wallet. This is the core identity-to-wallet relationship and should be verified before deployment.

NAMED-PERSON SUB-VAULTS

- Typical roles may include SPOUSE, CFO_PARTNER, TRUSTEE or BENEFICIARY.
- Each named person requires an individual genomic sequence, individual GIS and dedicated source wallet.
- Named-person vaults do not inherit the authority of the Main Vault simply because they are part of the same family or institutional structure.

UNASSIGNED AND UNDER-18 STRUCTURES

- Unassigned / Main-GIS sub-vaults remain listed under the Main Vault GIS and retain Main Vault control.
- Under-18 beneficiaries operate in Escrow Mode under the Main Vault GIS until the contract-defined transition point.

PRE-DEPLOYMENT CHECK

Confirm every intended identity, role, source wallet and beneficiary relationship before the contract is deployed.

2. TRANSFER AUTHORITY & TRANSACTION RATE LIMITS

Transfer authority is intentionally asymmetric. The Main Vault governs horizontal movement across the ecosystem, while individual named sub-vaults are constrained to their own designated source-wallet path.

MAIN VAULT GIS Horizontal authority	**SUB-VAULT** Vertical authority only	**SOURCE WALLET** Designated destination
Main Vault ↔ configured sub-vaults	Own sub-vault → own source wallet	Receives only from its mapped vault

MAIN VAULT TRANSFER RULE

- The Main Vault GIS is the only horizontal transfer authority.
- The Main Vault may move assets between the Main Vault and configured sub-vaults.
- Transfers from the Main Vault into any individual sub-vault are capped at 3 per calendar year.
- With 10 sub-vaults, the theoretical aggregate ceiling is 30 such transfers per year, subject to the deployed configuration.

NAMED SUB-VAULT RULE

- A named sub-vault is limited to vertical transfers to its own designated Sub-Vault Source Wallet.
- No cross-vault access is intended between named sub-vaults.
- The source-wallet relationship should be validated before funding.

WHY THIS MATTERS

The transfer policy creates a clear distinction between **governance authority** and **asset destination authority**. A signer or operator should not assume that possession of a host-wallet credential automatically creates authority to move assets between isolated sub-vaults.

OPERATOR CHECK

Record the expected annual transfer pattern and confirm that it is compatible with the configured rate limits before deployment.

3. LOCK MODE GOVERNANCE

Lock Mode provides a deliberate governance mechanism for temporarily freezing sub-vault activity while preserving Main Vault control.

STANDARD MODE	LOCK MODE
Sub-vaults may execute their permitted transfer path to designated source wallets.	Sub-vault transfers are frozen. Main Vault operation remains available under the configured rules.
Primary use: normal operating conditions	**Primary use:** controlled pause during governance, security or estate-processing conditions

MAIN VAULT AUTHORITY

- The Main Vault GIS can place the ecosystem into Lock Mode.
- The purpose is to create a controlled pause in sub-vault transfers without removing Main Vault oversight.

AUTOMATIC UNLOCK ON LIQUIDATION EVENT

If the configured liquidation event occurs, Lock Mode is designed to drop automatically so estate processing can proceed under the succession rules.

OPERATIONAL CONSIDERATION

Lock Mode should be treated as a governance control, not as a substitute for incident response, legal authority or estate administration. Institutions should document who is authorized to invoke it and under what internal circumstances.

CONTROL PRINCIPLE

Pause movement without surrendering oversight. The Main Vault remains the governing layer while sub-vault activity is constrained.

PRE-DEPLOYMENT QUESTIONS

- Who is authorized to invoke Lock Mode?
- What internal event would justify its use?
- How will the family, trustee or operations team document the decision?
- Who is responsible for monitoring the configured inactivity window?

4. SUCCESSION ORDER & AUTOMATIC LIQUIDATION EVENT

Succession is designed to be rule-based rather than dependent on an operator manually reconstructing authority after a prolonged period of inactivity.

DAY 0	DAY 365	+30 DAYS	DAY 395
Last valid keepalive signature	Inactivity threshold reached	Grace period	Liquidation event

LIQUIDATION EVENT

A liquidation event is triggered when there is no keepalive signature within the configured 365-day inactivity window followed by a 30-day grace period, producing a total technical window of 395 days.

IMPORTANT GOVERNANCE DISTINCTION

For the contract, inactivity, incapacity and passing may be technically equivalent trigger conditions. This should **not** be interpreted as a legal determination of death or incapacity. Legal and estate procedures remain separate.

EVENT SEQUENCE

- Lock Mode drops automatically when the liquidation event occurs.
- Assets are redistributed uniformly / pro-rata according to the configured allocation basis points.
- The configured successor priority is applied.

SUCCESSOR PRIORITY

1	CFO / CLO / PARTNER
2	TRUSTEE
3	SPOUSE

The intended design is for the succession order and allocation logic to be hardcoded into the deployed configuration. Because these rules can become operationally consequential, the configured recipients and allocation basis points should be independently checked before activation.

5. CONTRACT IMMUTABILITY, EXPIRATION & RECONFIGURATION

The AVEUM governance model treats deployed configuration as a long-lived control surface. The central operational principle is simple: review the rules carefully before deployment because post-deployment changes may not be available.

LICENSE PERIOD	DEPLOYED CONFIGURATION	END OF TERM
5 or 10 year term, according to the selected license.	Configuration is locked on-chain and intended to be immutable for the term.	Old contract expires and the configured reconfiguration sequence can begin.

IMMUTABILITY

- User, administrator or AVEUM operator should not be assumed to have the ability to alter locked configuration.
- Automatic renewal is intended to preserve the configured rules rather than silently change them.
- The governance, transfer and succession settings should therefore be reviewed as if they will remain fixed.

RECONFIGURATION AT LICENSE END

- The old contract expires.
- Assets sweep to the Old Source Wallet under the configured process.
- A new license is established with a new GIS and new architecture.
- Assets move from the old source to the new source according to the reconfiguration procedure.

THE PRE-DEPLOYMENT PRINCIPLE

Absolute immutability increases the value of pre-deployment review. Treat every role, wallet mapping, transfer limit, inactivity period, successor and allocation rule as a material configuration item.

RECOMMENDED REVIEW GROUP

- Security / MPC operator
- Legal and compliance
- Estate / trust adviser
- Family governance representative
- Technical deployment owner

6. PRE-OPERATIONAL READINESS CHECKLIST

Use this checklist as the final governance gate before entering the genomic testnet vault ecosystem. The objective is to eliminate avoidable ambiguity before immutable configuration is deployed.

1	**Identity mapping** Every GIS identity has been reviewed and matched to the intended person or role.	■
2	**Source wallets** Every dedicated source wallet has been independently verified.	■
3	**Main Vault authority** The person / governance body responsible for Main Vault GIS control is documented.	■
4	**Sub-vault roles** Named-person roles and beneficiary relationships are confirmed.	■
5	**Under-18 arrangements** Escrow Mode expectations and legal-age transition requirements are documented.	■
6	**Transfer limits** The 3-per-calendar-year Main Vault-to-individual-sub-vault rule has been reviewed.	■
7	**Lock Mode** Internal authorization to invoke Lock Mode is documented.	■
8	**Succession** CFO/CLO/PARTNER, TRUSTEE and SPOUSE priority is intentionally configured.	■
9	**Allocation basis points** The intended pro-rata allocation is checked and signed off.	■
10	**Inactivity window** 365 days + 30-day grace period is understood and accepted.	■
11	**Legal distinction** All parties understand that technical inactivity triggers are not legal determinations.	■
12	**Immutability** The final configuration has been reviewed on the assumption it cannot be changed during the license term.	■
13	**Testnet scope** All testnet assets and data are understood to be non-production / synthetic unless expressly stated otherwise.	■
14	**Incident response** Security, custody and governance escalation contacts are documented.	■

Deployment gate: do not proceed until all material governance items are reviewed and the final configuration is approved by the appropriate stakeholders.

7. IMPORTANT DISCLOSURES & TESTNET SCOPE

This document is an operational orientation guide. It is not a substitute for independent technical review, legal advice, compliance review, estate planning or fiduciary oversight.

Testnet scope

The guide is intended for the AVEUM genomic testnet vault ecosystem. Testnet environments and assets should not be treated as production custody unless expressly designated.

Security scope

No architecture eliminates all security, operational, governance, legal or human risk. AVEUM should be evaluated as an additional vault security and governance layer alongside institutional custody controls.

Host-wallet compromise

The architectural objective is that compromise of a host wallet does not, by itself, authorize access to an isolated Family Vault. This should be understood as a design objective subject to the deployed contract, identity controls and implementation.

Technical liquidation trigger

The 395-day inactivity sequence is a technical contract trigger. It is not a legal determination of death, incapacity or estate entitlement.

Immutability

Where configuration is immutable for the license term, mistakes can be consequential. Review identities, wallets, transfer limits, succession priority and allocations before deployment.

Independent review

Smart-contract behavior is governed by deployed code and configuration. Independent security, legal, compliance and estate review is recommended before production use.

Advice disclaimer

Nothing in this document constitutes legal, tax, investment, fiduciary, estate-planning or financial advice.

REFERENCE POINT

For current protocol architecture, institutional integration information and the latest AVEUM materials, consult the official AVEUM documentation and deployment environment.

Document status: Pre-operational reference | Prepared for governance review | Version 1.0