**Emergency Governance Rollback Policy: Synergy Network**

**1. Introduction**

This document defines the emergency rollback mechanisms for the Synergy Network in the event of governance or security failures. It ensures resilience by providing structured procedures to halt, review, and restore network operations while maintaining decentralization and security integrity.

**2. Multi-Signature Emergency Stops**

**2.1 Definition & Use Cases**

* Multi-signature (multi-sig) controls are implemented to enable authorized parties to pause network operations in case of security breaches or governance failures.
* Applicable scenarios include:
  + Detection of severe smart contract vulnerabilities.
  + Network governance takeover attempts.
  + Mass Sybil attack incidents.
  + DDoS-induced network instability.

**2.2 Multi-Sig Thresholds**

* A **3-of-5** or **5-of-7** multi-signature requirement is enforced for critical actions.
* Signers include **core validators, governance council members, and independent security auditors**.
* A multi-sig threshold decision automatically triggers an on-chain status change to **Paused Mode**.

**3. Reversion Procedures**

**3.1 Snapshot-Based Recovery**

* The network periodically generates **state snapshots** to allow a rollback to the latest stable state.
* **Criteria for rollback activation:**
  + Consensus among governance signers.
  + Community voting approval for major network state reversion.
* Upon rollback approval, the system reverts to the last stable snapshot before the attack or exploit occurred.

**3.2 Validator Intervention & Hard Fork Procedures**

* In case of governance failure, validators may invoke **emergency hard forks** to restore network integrity.
* A hard fork requires:
  + A **two-thirds majority consensus** among validators.
  + A **publicly-audited rollback justification**.
* Post-hard fork, the DAO governance council will initiate an independent review of system vulnerabilities.

**4. Governance Intervention Mechanisms**

**4.1 Temporary Governance Freeze**

* If governance manipulation is detected, emergency **voting freezes** prevent malicious actors from influencing further changes.
* A freeze is enforced if:
  + The governance council votes **75% in favor of temporary suspension**.
  + Automated anomaly detection flags governance exploits.
* Once governance is frozen, **a forensic audit of voting activities** is conducted before resuming normal operations.

**4.2 Community Emergency Referendum**

* In extreme cases, a **Community Emergency Referendum** may be triggered.
* This requires **at least 10% of active token holders** to propose and sign a referendum for urgent governance changes.
* The referendum passes if **60% or more** of the voting participants approve it.

**5. Compliance & Security Standards**

* All rollback measures align with regulatory compliance requirements, including **SEC, GDPR, and AML frameworks**.
* An independent **security review board** oversees rollback procedures to prevent misuse.
* Revisions to this policy are subject to **DAO voting approval** to maintain decentralized governance integrity.

**6. Conclusion**

The Synergy Network's emergency governance rollback framework is designed to balance security, decentralization, and operational resilience. By leveraging multi-signature emergency stops, validator-driven rollback mechanisms, and community engagement, the network ensures that governance and security failures are managed effectively while preserving trust and transparency.