Fail-Safe Protocol & Emergency Procedures

Critical Fail-Safe Protocol

1. System Lockdown (Circuit Breaker)

- **Trigger**: Detection of active brute-force attack, key compromise, or massive anomaly in AI Purifier.
- **Action**:
    1. Immediately reject all non-administrative traffic.
    2. Revoke current active session tokens.
    3. Notify Security Operations Center (SOC).

2. Key Compromise Protocol

- **Trigger**: Reported or detected leakage of a master key or signing key.
- **Action**:
    1. Execute **Automatic Key Rotation** immediately.
    2. Mark all data encrypted with the compromised key for "Re-Encryption Priority".
    3. Generate forensic report on usage of compromised key.

3. Auditor Integrity Failure

- **Trigger**: mismatch in hash chain validation of the Immutable Auditor.
- **Action**:
    1. System moves to **Read-Only Mode**.
    2. Alert "Critical Integrity Breach" to Compliance Officers.
    3. Halt all new write operations until manual verification.

Emergency Shutdown

- **Manual Override**: Physical or Hardware-backed multi-signature authorization required to completely shut down the SafeCore service.
- **State Preservation**: Ram content flushed to encrypted swap; keys cleared from memory.