🛡️ v008-OBSIDIAN — Sovereign Spec Sheet

Deterministic Thermal-Power Governance Engine for High-Density AI Silicon (1,000W+)

v008-OBSIDIAN is **not a cooling system** and does not replace facility thermal infrastructure. It is an independent **enforcement authority** that governs silicon operating envelopes in real time, ensuring hardware longevity, insurance compliance, and forensic accountability at extreme power densities.

⚡ Technical Specifications

Parameter	Specification	Notes / Standard
Target TDP Class	1,000W – 1,500W+ per accelerator	Designed for Blackwell-, Rubin-class GPUs and custom AI ASICs
Enforcement Latency	**< 20 ms**	Sub-thermal-timescale response
Observed Junction Stabilization	**~15°C – 20°C**	Observed under governed transient workloads vs. ungoverned operation
Governance Logic	Deterministic, physics-derived	Non-probabilistic boundary enforcement
Audit Artifact	Sovereign Enforcement Receipt	SHA-256 cryptographically chained ledger
Integration Mode	Out-of-band / sidecar	No access to AI models, weights, or training data

OEM Relationship	Augmentative	Does not bypass vendor safety limits

---

🛠️ Operating Effects & Stabilization

1. Thermal Overshoot Prevention

Conventional OEM thermal management is **reactive**, often permitting transient power spikes that exceed safe margins before throttling or cooling response occurs.

v008-OBSIDIAN enforces power and thermal boundaries *prior* to runaway, preventing sub-thermal-timescale overshoot events that drive immediate silicon stress and long-term degradation.

---

2. Cumulative Thermal Fatigue Mitigation (Miner's Rule)

High-TDP silicon failure is frequently driven by **repeated transient excursions**, not steady-state temperature alone.

v008-OBSIDIAN stabilizes junction behavior during burst workloads, reducing both:

- the **frequency** of thermal cycles
- the **amplitude** of temperature deltas

Resulting Effect (observed, non-guaranteed):

- Lower cumulative fatigue accumulation
- Improved Mean Time Between Failures (MTBF) assumptions in high-utilization clusters

---

3. Forensic Receipting & Non-Repudiation

Every enforcement decision generates a **Sovereign Enforcement Receipt**.

- **Cryptographically chained (SHA-256)**
- **Tamper-evident by design**
- Independent of operator and silicon vendor

Any attempt to bypass, modify, or suppress governance actions permanently breaks the receipt chain, **invalidating governed status** for warranty or insurance purposes.

🌐 Compliance, Privacy & Deployment Architecture

- **Black-Box Operation:**
  Processes only physical telemetry (power, junction temperature, clock frequency).
- **IP Protection:**
  No access to AI weights, code, datasets, or internal network logic.
- **Infrastructure Compatibility:**
  Valid across liquid-cooled, air-cooled, and hybrid environments where physics permits.
- **Insurance & Regulatory Alignment:**
  Provides objective evidence suitable for:
  - Professional Liability (E&O)
  - Technology Property
  - Parametric Insurance triggers
  - GDPR / CCPA / PIPL audit requirements
  - SOC 2–aligned control environments (audit readiness)

📌 Risk Classification Impact

Deployment of v008-OBSIDIAN enables facilities to move from:

“High-Density Unmanaged Risk” → “Governed Infrastructure System”

Supporting:

- Preferred risk pricing
- Reduced claims ambiguity
- Improved subrogation outcomes
- CAPEX flexibility where physics-verified limits allow air or hybrid operation

---

Engineering & Risk Review

For deployment documentation, insurance review materials, or a **sample Sovereign Enforcement Receipt**, contact QH8 Risk Engineering.

Oleg Tatar
President & CEO, QH8 Technologies
📧 contact@qh8technologies.com
🔗 https://qh8technologies.com
📄 Technical Disclosure: https://qh8technologies.com/v008-obsidian

---