Privacy, Data Boundaries & Compliance

Technical Privacy Position for QH8 Infrastructure Governance

QH8 Technologies designs physical-layer infrastructure governance systems that operate without requiring unnecessary access to customer intellectual property, proprietary software, internal network logic, or confidential operating data.

Our approach is based on a simple principle:

Infrastructure governance should not require unnecessary visibility into client systems.

QH8 focuses on the physical operating layer. Our systems evaluate infrastructure behavior through technical signals related to power, thermal performance, equipment state, load behavior, operating boundaries, and system stability.

QH8 does not require access to AI models, training data, source code, application logic, private business records, proprietary design files, or trade-secret operating methods.

This allows operators to generate defensible infrastructure evidence while preserving control over their data environment, software stack, and confidential business information.

---

1. Non-Invasive Governance Model

QH8 is not designed as a traditional software monitoring platform.

Conventional observability tools may require access to software environments, logs, applications, cloud accounts, internal systems, or network-level data. QH8 takes a different approach.

The QH8 governance model evaluates physical infrastructure behavior without requiring access to confidential software assets or proprietary business systems.

This model supports:

- **Data minimization**
  Only necessary physical telemetry is processed for infrastructure governance.

- **Client IP protection**
  Sensitive competitive assets remain outside the QH8 evidence boundary.
- **Reduced data exposure**
  The system avoids unnecessary access to business-confidential systems and regulated information.
- **Clear processing boundaries**
  The deployment scope defines what technical signals are processed and why.
- **Separation of concerns**
  Infrastructure evidence is kept separate from proprietary software, business records, and confidential operating logic.

QH8 does not require visibility into AI weights, model architecture, training datasets, customer code, proprietary algorithms, internal business logic, or confidential production systems.

---

2. Physical Telemetry Scope

QH8 governance is based on infrastructure-level technical signals.

Depending on deployment scope, these signals may include:

- Power behavior
- Thermal behavior
- Load patterns
- Equipment state indicators
- Operating boundary conditions
- Event timing
- Enforcement records
- Infrastructure stability indicators

The purpose of this telemetry is to evaluate infrastructure integrity, stability, efficiency, and compliance readiness.

QH8 does not use this telemetry to inspect customer software, reverse engineer proprietary systems, extract confidential commercial information, or access regulated personal data outside the agreed deployment scope.

---

3. Evidence Integrity and Audit Support

QH8 can generate tamper-evident operational records for infrastructure events, enforcement activity, and physical-state review.

Where applicable, records may be sealed using cryptographic methods such as SHA-256 hashing and chained evidence receipts. This helps preserve the integrity of the evidence record from observed infrastructure behavior to final report output.

These records may support:

- Insurance review
- Warranty review
- Investor and lender due diligence
- Infrastructure audit preparation
- Compliance documentation
- Export-related technical evidence review
- Loss attribution analysis
- Operational risk review

QH8 evidence records are designed to reduce ambiguity after an operational event by preserving a structured and reviewable record of physical infrastructure behavior.

---

4. Data Sovereignty and Processing Boundaries

QH8 is designed for clients operating across jurisdictions with strict data-control requirements.

The system is built around the following processing principles:

- Process only the telemetry required for infrastructure governance
- Avoid access to regulated personal data unless explicitly required by the deployment scope
- Avoid access to proprietary software and customer intellectual property
- Preserve separation between operational evidence and business-confidential data
- Support documentation of what data was processed and why
- Keep deployment-specific data handling terms defined in the applicable customer agreement

QH8’s governance model is designed to support privacy-conscious infrastructure review without expanding unnecessary data exposure.

---

5. Regulatory and Control Alignment

QH8 is not a replacement for a client's legal, privacy, cybersecurity, or compliance program.

However, the QH8 architecture is designed to support common compliance principles found in modern privacy, security, audit, and infrastructure-risk frameworks, including:

- Data minimization
- Purpose limitation
- Access limitation
- Auditability
- Evidence integrity
- Operational accountability
- Infrastructure risk governance

Where required, QH8 documentation can support customer review processes related to internal controls, insurance underwriting, investor due diligence, technical compliance preparation, and infrastructure-risk assessment.

QH8 does not claim that use of its system automatically satisfies any specific regulatory regime. Compliance obligations remain dependent on the client's jurisdiction, deployment model, contractual requirements, and legal review.

---

6. Hardware Integrity and Safety

QH8 does not replace OEM safety systems, equipment protection logic, manufacturer-defined operating controls, or site-level safety procedures.

QH8 is designed to augment infrastructure governance by identifying and managing physical operating boundaries before instability becomes a failure event.

This may support review of:

- Thermal stress
- Power instability
- Repeated transient excursions
- Degradation risk
- Abnormal operating patterns
- Infrastructure overload conditions
- Boundary violations and enforcement events

The objective is to improve operational discipline, preserve asset integrity, and create defensible evidence of how infrastructure behaved under real-world operating conditions.

---

7. Client Intellectual Property Protection

QH8 does not require clients to disclose proprietary system architecture, confidential production logic, source code, AI models, customer datasets, internal business systems, or trade-secret operating methods.

The client remains responsible for controlling its proprietary information, access permissions, data retention policies, and internal compliance requirements.

QH8's role is to provide a physical-layer governance and evidence system that can operate without unnecessary exposure of client intellectual property.

---

8. Important Notice

This document is a technical privacy and compliance overview.

It does not replace a formal privacy policy, data processing agreement, cybersecurity assessment, regulatory filing, legal opinion, customer-specific compliance review, or contractual security addendum.

Deployment-specific data handling, retention, access control, processing terms, evidence ownership, and review rights should be defined in the applicable customer agreement, statement of work, data processing documentation, or service documentation.

QH8 Technologies
Contact: contact@qh8technologies.com
Website: https://qh8technologies.com