Loggie

Security & Risk FAQ

Defense & Regulated Environments

Is this blockchain?

No.

Loggie is an integrity layer that anchors cryptographic commitments. It can optionally notarize root commitments to a third-party timestamping layer, but blockchain is not required for operation.

All core integrity functions operate independently of any public network.

Does any operational data leave our network?

No.

Loggie does not transmit logs, telemetry, documents, or AI outputs outside the customer environment. Only cryptographic commitments (hashes) may optionally cross a controlled boundary. These commitments cannot reconstruct source data.

Who controls cryptographic keys?

The customer.

Key material can be generated, stored, and managed entirely within the customer-controlled environment. Loggie does not require external custody of private keys. Deployment supports integration with internal HSM or key management systems where required.

What happens if we disconnect from the anchor layer?

Nothing operationally.

Loggie continues to hash, batch, and verify records internally. Optional external notarization can resume at any time. No historical integrity is lost.
The anchor layer is additive, not foundational.

Can it operate in an air-gapped environment?

Yes.

All core functionality — hashing, batching, identity binding, verification — operates fully internal with no external connectivity required. Air-gapped deployment is a supported model.

Is it export controlled?

Loggie uses commercially available cryptographic primitives. Export classification depends on deployment configuration and jurisdiction. No specialized defense-restricted cryptographic algorithms are required for operation. (Provide ECCN determination separately if needed.)

Does Loggie introduce operational risk?

No new data exposure surfaces are created.

Loggie does not ingest or centralize sensitive data beyond cryptographic commitments.
It operates as a verification layer adjacent to existing systems.

Is Loggie a system of record?

No.

Loggie does not replace storage systems, SIEMs, or databases. It establishes independent integrity over records generated by those systems.

Additional documentation available upon request: NIST mapping, CMMC control alignment, key management posture, threat model overview.