

SECURITY MEASURES

Security measures

This is the technical summary, written for whoever reviews suppliers on your behalf. It states what is in place, how each measure is verified, and what is not in place. Nothing here is aspirational.

Version 1.0 · Date 20 September 2026 · Status Approved for release — 12 October 2026 · For Your IT adviser

Summary of controls

Area	Measure	Status
Data at rest	LUKS2 full-device encryption, AES-XTS-512, argon2id key derivation	In place
Key management	Passphrase held in the director's memory only. No keyfile, no auto-unlock, no escrow.	In place
Access control	Single named individual. No employees, contractors or third parties.	In place
Session handling	Storage unlocked per working session, locked afterwards	In place
Data egress	Processing pipeline contains no network code and cannot transmit data	In place
Audit logging	Append-only, hash-chained record of automated actions	In place
Incident notification	Client notified without undue delay, with supporting information	In place
Certification	ISO 27001, Cyber Essentials	Not held
Cyber insurance	Professional indemnity, cyber liability	Not held

Encryption at rest

Client data is held on a removable solid-state device encrypted in full with LUKS2. The header parameters, as dumped from the device, are:

FormatLUKS2 Cipheraes-xts-plain64 Key size512 bits Key derivationargon2id ScopeEntire device, including filesystem metadata

You may verify this yourself: the header dump can be produced on request. It is also retained for each engagement as the record proving data was encrypted before destruction.

Key management

The passphrase exists only in the director's memory. We have verified the absence of every mechanism by which a key could otherwise be available:

no keyfile exists anywhere on the system;

the boot-time encryption table is empty, so the volume cannot unlock at startup;

there is no mount entry for it;

no system service unlocks it;

the passphrase is not written to disk, escrowed, or held by any third party.

The practical consequence: theft of the machine yields nothing. There is no configuration in which the data is readable without a person typing the passphrase.

Data egress

The pipeline that reads and structures client documents runs locally and contains no networking code. It cannot transmit data, because there is no code path that could.

This is architecturally different from the usual arrangement in AI document processing, where documents are sent to a third-party model provider. We do not do that with client records.

Audit logging

Automated actions are written to an append-only log. Each entry is cryptographically chained to its predecessor, so any alteration or removal is detectable. The log records the action, timestamp and session — not the contents of client data — and credential-shaped values are redacted before being written.

The log is not shipped to any external service. It resides on the same encrypted hardware as the work.

Automation limits

Work is executed by autonomous software under the director's control. It cannot send anything outside our systems, delete files, alter system configuration, or incur cost without the director's explicit confirmation for each occurrence. Full detail is in How our AI is governed.

Separation from client systems

We work on our own hardware, not yours. We do not require access to your network, your email, or your infrastructure, and we do not install software on your systems. Data is transferred by agreement, processed on our encrypted device, and returned.

Incident response

If we become aware of a breach affecting your data, we notify you without undue delay and give you the information you need to meet your own obligations under Articles 33 and 34. We do not wait for a full investigation before telling you something has happened.

What is not in place

A security summary that lists only strengths is marketing. The gaps:

No ISO 27001 certification. No formal information security management system.

No Cyber Essentials certification. We meet several of the controls but have not been assessed.

No cyber liability or professional indemnity insurance. This is a live decision.

No independent penetration test or code audit. The attack surface is small — one encrypted device, one person, no external services — but no third party has tested it. Everything we assert about the pipeline is self-attested.

No key recovery of any kind. The passphrase exists only in the director's memory. There is no keyfile, no escrow and no split-key arrangement. If the director dies or is incapacitated during an engagement, your data is permanently unrecoverable — we would be unable to return it, and unable to destroy it. This is a deliberate confidentiality choice with a serious availability consequence, and it is the single largest risk in this document.

No DMA protection. The machine has no Thunderbolt port, which removes the usual attack path, but IOMMU is not enabled, so hardware DMA is not remapped. A malicious device connected during an active session is a theoretical route to memory.

Keys are in memory while the volume is open. Disk encryption protects data at rest, not a running machine. While unlocked, the key is in RAM, and the volume can be left open if a session is not closed. Closing the lid suspends the machine without locking the volume.

The agent has full access during a session. It cannot unlock the volume and cannot lock it, but while the director holds it open the agent can read and write without restriction. See How we handle your data.

No business continuity arrangement beyond one person. If the director is unavailable, work stops and there is no documented succession.

We would rather you knew these before your due diligence finds them.

Questions

Technical questions to info@inferencesystems.co.uk. We will produce evidence rather than assertions.

Inference Systems Ltd — registered in Scotland, company number SC903263. Registered office: 116 Peggieshill Road, Ayr, Scotland, KA7 3RA. info@inferencesystems.co.uk