Bracton

Case and client management, with the work already done.

INFORMATION SECURITY

Information security policy

DOCUMENT	BRL-IS-001, version 1.2
DATE	September 2026
APPLIES TO	The Bracton platform, the Bracton AI Assistant, and the systems Bracton Ltd runs to operate them
OWNER	Saqib Khan, Director
REVIEW	At least annually, and after any security incident or material change to the platform

Bracton Ltd, a company registered in England and Wales, number 17360622
Registered office Arden Hall, Brooklands Road, Sale, M33 3SJ
bractonlegal.co.uk

Bracton holds live matter files, privileged correspondence, anti money laundering evidence and the client and office ledgers a firm keeps under the SRA Accounts Rules. Your firm carries the regulatory consequence if that content leaks, so this policy is written to be tested rather than believed.

i. Why this policy exists

Bracton holds the content of live client matters. That includes correspondence subject to legal professional privilege, medical and other health records, the evidence a firm gathers for anti money laundering purposes, and the client and office account ledgers a firm keeps under the SRA Accounts Rules. It is among the most sensitive material a small business handles anywhere, and the firm that puts it into Bracton carries the regulatory consequence if it is lost or disclosed.

So the security position was written before the first line of code rather than assembled once a buyer asked for it. The full detail sits in the Bracton Security and Hosting Specification, which forms part of the data processing agreement and which any firm can read during due diligence. This policy states the position that specification commits the company to.

> Every control below is a requirement on the build and a term the company contracts to before a firm signs.

ii. Where the responsibility sits

Your firm is the controller. It decides why client personal data is processed and to what end, it owes the duty of confidentiality to its clients, and it answers to the Solicitors Regulation Authority for how client money and client information are looked after. Buying software moves none of that. A firm that suffers a breach through its supplier is still the firm the Information Commission writes to, and the compliance officer for legal practice is still the person who has to judge whether the SRA needs to be told.

Bracton Ltd is the processor. It acts on your documented instructions and for no other purpose, it does not decide what your data is used for, it does not use your matter content for its own product development, and it does not disclose that content except where you instruct it or the law compels it. Because your firm cannot delegate its own obligation, it is entitled to verify rather than accept, and everything set out below is written so that it can be tested.

iii. Where a firm's data is held

All production data is stored and processed in the United Kingdom. That covers the database, which holds the papers and their files as well as the records, the backups, the audit trail and every queue or cache that carries matter content at any point.

The places this goes wrong in practice are rarely the database. Error tracking, application monitoring, log aggregation, support tooling and analytics all tend to send their payloads to whichever region a vendor defaults to, and those payloads routinely carry fragments of the content that caused the event. Each such service is configured to a United Kingdom region, excluded outright, or configured to strip content before it transmits, and the position for each one is recorded so that a firm reads the working rather than the conclusion.

Reaching United Kingdom data from outside the United Kingdom is a transfer even where the data itself stays put. Support and engineering are United Kingdom based, and any exception, including a contractor working from abroad, is recorded in the record of processing and disclosed to firms before it happens rather than treated as an internal detail.

> The hosting provider for a paying firm and the specific United Kingdom regions are not chosen. A host in the London region serves the demonstration. The choice for a paying firm will be made against this requirement and both will be named to firms before signature.

iv. One firm kept from another

Application code contains mistakes. A query written without a filter for the firm, a caching layer keyed on the wrong value, an endpoint that trusts an identifier out of the request, each is an ordinary defect and each would be serious here. So the separation between firms is enforced underneath the application, in the database itself.

Each firm has a database of its own, so no table carries a column naming the firm and no rule has to be remembered to keep one firm's rows away from another's. A query that forgets which firm it is asking about reaches the control database, finds no such table there and fails loudly, so the worst outcome of that class of mistake is a broken screen and an alarm rather than a disclosure. A paper's files are bytes in that same database beside the paper they belong to, rather than objects in a separate store, so custody, the hourly backup and destruction at the end of retention all travel together, and every file is served through one door that asks who is asking and refuses a person the file's own barrier excludes.

An address of its own for each firm, rather than one shared address, is designed and not yet built. A session token turning up at the wrong address would be refused rather than examined, an unfamiliar sign in address is a visible wrong note to the people who use it, and the arrangement pairs with passkeys, which bind to the address they were

created for. bracton.app is held for it and it goes in with the production host. Today there is one address.

This is tested rather than asserted. An automated suite signs in as one firm and attempts to reach another firm's matters, documents, ledgers and audit records through every route the product exposes, and separately attempts the same directly against the database using the application's own role. A single record returned fails the build, and the suite runs on every change, because this is the control most likely to be broken quietly by a refactor.

> This is separation between firms. It is not separation between the office and the hotel, and it will not be sold as though it were.

v. Encryption, and who holds the keys

Traffic between a fee earner and the product is encrypted in transit using current transport security, with older versions refused rather than tolerated. At rest, every backup is sealed under AES-256 with a key the platform holds and the hosting company does not, tested weekly by restoring one and recording the result either way. Encryption of the running database at rest is the hosting company's and is named here once the production host is chosen. There is no separate document store and no search index: a paper's files sit in the firm's own database and search queries that database's own tables.

The position on keys is stated plainly rather than aspirationally. Two keys exist, one sealing the backups and one guarding the mail tokens held in each firm's custody, both read from the server's environment. There is no key for each firm, no managed key service and no automatic rotation, so deletion at the end of a contract is evidenced by the firm's database being dropped and its backups expiring, recorded on the trail, rather than by a key being destroyed. A key for each firm in a managed service, rotated on a schedule and on suspected exposure, goes in with the production host, and this policy will say when it has.

> Whether a firm can supply and hold its own key material, so that Bracton Ltd cannot decrypt that firm's data without the firm's participation, is not settled. It is attractive to larger buyers and it complicates recovery, and the position will be settled before the first firm signs rather than left ambiguous in a contract.

vi. Who can reach a firm's data

Bracton is hosted, so a fee earner at a desk in your office reaches it over the internet in the same way as one working from a hotel. There is no separate remote access portal and there will not be one, because publishing a second front door creates a second thing to keep patched without creating a boundary. Trust attaches to the device instead.

A device your firm has registered is treated as known, and the person using it gets the whole application. A device your firm has not registered is treated as unknown whoever is sitting at it, and gets a session that times out after a short period of inactivity, caches nothing, refuses downloads and suppresses printing. It is a session for reading a file rather than for taking a copy of one. Registering and revoking devices are administrative acts your firm carries out on its own account, revoking a device ends every live session on it at once, and removing a person from the firm ends their sessions and their device registrations in the same action.

The factors are the passkey and the person. A passkey is a credential minted inside the person's own device and bound to the address it was created for, so nothing shared travels and a whole category of attack is removed rather than made harder, and the device is also required to prove the person holding it by face, fingerprint or its own PIN, insisted on when the passkey is registered, when a sign in is asked for and again when the device's answer is verified. No authenticator application is offered, because a six digit code reintroduces the shared secret a passkey exists to remove. Where a firm signs in through its own Microsoft directory the factors are that tenant's policy and remain the firm's to set. For the actions where the consequence is money leaving a client account or a document reaching the other side, the system demands the second factor again at the moment the action is approved rather than relying on a login four hours earlier. Those actions are approving a payment out of the client or office account, changing bank details already held, transferring between client and office account, releasing a bill, and serving or disclosing a document.

> Suppressing printing reduces bulk copying and does nothing to stop a person photographing a screen. It is a control against carelessness and casual theft rather than against a determined insider, and it is offered as no more than that.

vii. What people at Bracton Ltd can reach

Nobody at Bracton Ltd holds standing access to the production database. Development works against the application and against invented data, and reading live client material is not part of anyone's ordinary permissions. Where a fault genuinely requires it, access is requested in writing against a specific fault, limited to a short window that expires by itself rather than waiting to be removed, and recorded statement by statement. Where the access reaches an identifiable firm's data, that firm's administrator is told.

Here the size of the company has to be stated rather than glossed. The usual control is that a second person approves the request, and Bracton Ltd is one director with no employees, so there is no second person and the two person rule cannot operate today. What stands in its place is that every grant is written to an append only record the application cannot alter, that the affected firm is told when the access touched its data, and that unauthorised access is a breach of the agreement the firm can enforce.

Those are the controls that exist, and they are weaker than a second approver. When the company takes on a second person with production access, approval by somebody other than the requester becomes the rule and this policy will say so.

Everyone with any production access is vetted before appointment and holds confidentiality obligations that survive their leaving. Accounts at the hosting provider carry the same second factor requirements as the product, since an administrative account there reaches everything the product does and more.

viii. What the permission model does not do

This section exists because a firm is better served by being told than by finding out.

The permission model governs the application. It decides which matters appear in a fee earner's list, which files an information barrier conceals, who can post to the client account and who can approve a payment. Inside the application it is the control that does the work, and it is specified and tested as such.

Below the application it does nothing at all, because anyone with access to the underlying database reads everything regardless of what the permission model says. So it must never be offered to a firm as a technical guarantee that Bracton Ltd or its hosting provider cannot see that firm's files, because it is not that. What protects the data below the application is the controlled access procedure above, the logging of every use of it, the vetting and confidentiality obligations of the people who can ask, and a contractual position that makes unauthorised access a breach the firm can enforce. Those are process and legal controls, and they are the honest answer.

None of this is peculiar to Bracton. Every hosted system shares it, including the ones your firm already uses, and the difference between suppliers is whether they say so and what they put in its place.

ix. What is recorded

Most systems log what was changed. In a law firm the more revealing question is often who looked. A conflict is created by a person seeing a file, not by them editing it, and an information barrier is breached the moment somebody on the wrong side of it opens a document, with nothing about the file changing to show it. A firm that has to prove to a court, an insurer or the SRA that its barrier held needs a record of reads, and a system that logs only writes cannot give it one.

Bracton records reads of sensitive material with the same care as writes. Each entry carries the person, the act, the firm, the file or ledger record it touched and the moment, and beside those the particulars of the request, being the sitting, the device the firm vouched for, the network address, the browser and whether the act was done or refused. The sitting is named by a digest of its ticket rather than the ticket itself, so a

copied trail cannot be replayed as a sign in. Refusals are kept as carefully as successes, because a person repeatedly reaching for files they cannot open is one of the few signals that arrives before the damage, and every refusal a person meets is written with the words they read and the door they were at. Work done by the platform's own timers carries no such particulars, and the absence says so.

The log is append only, written to a store the application's own role can add to and cannot alter or delete, so a compromise of the application does not let an attacker erase the trail. One pattern raises an alert today rather than sitting in a file nobody reads, being one person meeting many refusals in a day, which is what somebody reaching for what they may not have looks like from the outside, and further patterns join it as they are built rather than being promised here. A firm's administrator searches the trail from the search screen and exports the whole of it from Settings without asking, because a compliance officer producing evidence to a regulator cannot be waiting on a support ticket.

> The default retention period for the audit log, and the range a firm can set, are not settled. Both will be fixed before the first firm signs, because a firm's own retention policy and its insurer's requirements decide the right answer.

x. Backups, and restores that have been tried

Backups are immutable for a defined period, meaning that once written they cannot be altered or deleted before that period expires by anyone, including an administrator of the hosting account and including Bracton Ltd. This is the control that decides whether a ransomware incident is a bad week or the end of a firm, because the first thing competent attackers do is delete the backups, and a backup a compromised account can delete is not a backup.

Copies are held apart geographically in a separate United Kingdom facility, so that the loss of one site does not take the data and its safety copy together, and they do not leave the United Kingdom to achieve that separation.

Restores are tested rather than assumed, into a clean environment, with the time taken and the result recorded. The tests include restoring a single firm and not only the whole platform, because the incident that happens in practice is one firm losing a folder of documents to a mistaken deletion, and a process that can restore only everything is useless in that case.

> The contractual recovery point and recovery time objectives are not settled. A figure in a contract the architecture cannot meet is worse than no figure at all, so they will be set before the first firm signs.

xi. Certification, stated plainly

Certification does not make a system secure. It evidences that a defined set of controls exists and has been examined by somebody independent, which is a different and more modest claim. It matters here for a commercial reason, because a firm's professional indemnity insurer, its lender panels and its larger clients ask what a supplier holds.

The systems this policy governs are certified to Cyber Essentials. Bracton Ltd holds a certificate of assurance in its own name, number ef2524f2-b1ad-4d5f-bfb2-0702fa956a88, awarded by IASME on 5 August 2026, assessed against version 3.3 of the scheme with the whole organisation in scope, and due for recertification on 5 August 2027. The certificate is verifiable on the register and its face records that it is the child of a parent certificate, because the devices, accounts and Microsoft 365 tenant used to build and operate the platform are provided by an associated company with the same sole director and registered office, and the scheme certifies the two together with Bracton Ltd assessed in its own right. Bracton Ltd claims no more than that certificate says, and the assessment report evidencing the scope is available on request.

The path from here is Cyber Essentials Plus, then ISO 27001 once the product is live and there is an operating history for an auditor to examine, because certifying a management system that has not yet operated produces a certificate and not much else. No target date is committed. Certification carries the cyber cover IASME attaches to it, underwritten by American International Group UK Limited, insuring Bracton Ltd under its own certificate to a limit of twenty five thousand pounds in the aggregate including defence costs and running to 5 August 2027, as the certification body confirmed in writing on 10 September 2026. That cover is not the technology errors and omissions and cyber cover the software agreement requires of Bracton Ltd before a firm signs, which is dealt with in the business continuity policy and is not yet bound.

Independent penetration testing is a requirement rather than an option. The product is tested by an external party before the first firm goes live and at least once a year afterwards, with the separation between firms and the authentication flow expressly in scope, and the summary letter is available to firms during due diligence.

xii. If something goes wrong

Detection comes from monitoring rather than from a firm noticing. On confirming an incident, Bracton Ltd establishes what happened, which firms are affected and what categories of data are in scope, and contains it before investigating the cause.

Affected firms are told within twenty four hours of Bracton Ltd becoming aware, and sooner where the facts are already clear. That period is deliberate. Your firm has

seventy two hours from becoming aware to notify the Information Commission where the breach is likely to result in a risk to people's rights, and a supplier who takes two of those three days leaves the firm to make a regulatory filing on incomplete facts. Where the whole picture is not available inside twenty four hours, the notification goes out with what is known, says what is not yet known, and is updated at least every twelve hours until the position is stable.

Bracton Ltd then supplies the evidence your firm needs for its own reports, being extracts from the audit log, the list of affected records and a timeline the firm can attach to a filing, at no charge. Your firm decides whether to notify the Information Commission and whether to tell the people affected, because the obligation belongs to the controller and the judgement of risk is the firm's to make. The COLP's separate duty to report a serious breach to the SRA runs on a different test and a different timescale, and Bracton Ltd supplies the same evidence for that purpose without offering a view on whether the threshold is met.

xiii. What is not settled

A policy that fills its gaps with plausible answers is worse than one that names them. The following are open at the date of this policy, and each will be settled before a firm is asked to sign.

1. The hosting provider for a paying firm and the specific United Kingdom regions for production and for the separated backup copy, a host in the London region serving the demonstration meanwhile.
2. Whether United Kingdom only processing of matter content by the model provider is a setting for each firm or the single default. The provider itself is contracted and named on the sub processor list a firm reads during due diligence.
3. Whether a firm can supply and hold its own key material.
4. The contractual recovery point and recovery time objectives.
5. The default retention period for the audit log, and the range a firm can set.
6. The timing of the certification path, on which no date is committed.
7. Whether text message second factors are offered at all for ordinary login.
8. The application domain, which is separate from the marketing domain and not yet chosen.

xiv. Ownership and review

This policy is owned by the director of Bracton Ltd, who is accountable for the standards it sets. It is reviewed at least once a year, after any security incident, and whenever the platform changes in a way that affects a control described here. Where an open item above is settled, this policy is updated and the version raised.

Questions about anything in it go to hello@bractonlegal.co.uk, and a question a firm's compliance officer asks that this policy does not answer is treated as a defect in the policy.

This document is published at bractonlegal.co.uk/policy-information-security.html and the page carries the same words. Where a firm needs a position it does not state, write to hello@bractonlegal.co.uk and the answer goes into the next version.

Bracton Ltd, a company registered in England and Wales, number 17360622. Registered office Arden Hall, Brooklands Road, Sale, M33 3SJ.