BARBOURNE BROOK CUSTOMS PLANNING

SECURITY OVERVIEW FOR IT AND PROCUREMENT

CAT360 SECURITY AND DATA HANDLING SUMMARY

A standalone customs analytics service. No software to install, no connection to your network, and no access to your systems.

SERVICE IN SCOPE	INTEGRATION REQUIRED	DATA RESIDENCY	ISSUED
CAT360 (SaaS)	**None**	**London, UK**	**August 2026 · v1.1**

1 PURPOSE OF THIS DOCUMENT

This document sets out how CAT360 is delivered, what data it holds, where that data sits and what protects it. It is written for IT, security and procurement teams reviewing CAT360 as part of a purchase decision.

Most vendor security assessments are designed for software that connects to your estate: applications installed on your servers, agents running on your endpoints, or integrations that reach into your systems. CAT360 does none of these things. The great majority of a standard assessment is therefore not applicable, and we have set out below exactly why.

- **No integration with your systems.** CAT360 is accessed through a web browser. Nothing is installed, no network connection is made to your environment, and Barbourne Brook holds no accounts, roles or administrative access inside your estate.
- **No inbound access required.** We do not need firewall changes, VPN tunnels, site-to-site links, service accounts, directory access or open ports. If your users can reach a website, they can use CAT360.
- **Your data stays in the United Kingdom.** Primary processing and storage is AWS eu-west-2 (London). Personnel at Barbourne Brook have no physical access to any infrastructure holding your data.
- **Limited, low-sensitivity data.** The service holds customs declaration data and business contact details. It holds no cardholder data, no financial account data and no special category personal data under UK GDPR.
- **A live, evidenced security programme.** Controls are documented, findings are tracked to closure in a risk register, and a full completed vendor security questionnaire is available on request.

2 WHAT CAT360 IS AND HOW IT IS DELIVERED

CAT360 is a customs analytics platform provided by Barbourne Brook Ltd as software as a service. It analyses a business's own import and export declaration data to identify duty overpayments, classification errors, missed preference claims and compliance risk.

Delivery model	Multi-tenant software as a service, hosted and operated entirely by Barbourne Brook. Nothing runs in the customer environment.
How users access it	Standard web browser over HTTPS. There is no desktop client, no mobile application, no browser extension and no plug-in.
Where it runs	Amazon Web Services, eu-west-2 (London), with a managed SingleStore database.
Who operates it	Barbourne Brook engineering staff only. All development is carried out by Barbourne Brook employees.
Customer separation	Enforced at the application and data layer. Every query is scoped to a single customer, with role-based access control within the application.
Vendor access to your estate	None. We hold no accounts, no administrator roles and no standing access of any kind within customer systems.

3 WHAT CAT360 DOES NOT REQUIRE FROM YOUR IT ENVIRONMENT

The following are the items that most commonly drive a full IT assessment. None of them apply to CAT360.

No software installation
Nothing is deployed to your servers, desktops, laptops or mobile devices.

No network connectivity
No VPN, no site-to-site tunnel, no leased line and no firewall rule changes.

No inbound access
We never connect into your network. All traffic is outbound from your users' browsers to our service.

No directory integration
No Active Directory, LDAP or Entra ID connection, and no service accounts in your tenant.

No administrative rights
No local admin, no domain admin and no privileged accounts held by Barbourne Brook.

No endpoint agents
No monitoring agent, collector or data connector running on your machines.

No API into your systems
CAT360 does not call your applications, databases or middleware.

No data on your estate
The service is browser-accessed and cloud-hosted. Nothing is cached or stored locally by design.

No removable media
No USB devices, discs or tapes form any part of the service or its backups.

No payment data
CAT360 does not receive, process, store or transmit cardholder data. PCI DSS does not apply.

No special category data
No health, biometric or other Article 9 data is processed. Verified by field-level review in June 2026.

No secondary use of data
Your data is used solely to deliver the contracted service. It is never sold, pooled or reused.

What this means in practice. A compromise of CAT360 could not be used as a route into your network, because no such route exists. The risk to assess is confined to the confidentiality of the declaration data you choose to share with us, which is addressed in sections 4 to 8.

4 HOW YOUR DATA REACHES US

There are two routes into the service. Neither involves a technical connection to your systems.

ROUTE 1

You upload it

An authorised user at your business signs in to CAT360 and uploads declaration data through the browser over an encrypted connection. You choose what to share and when. No system-to-system link is created.

ROUTE 2

We obtain it from HMRC

Where you authorise us to do so, we obtain your CDS (Customs Declaration Service) declaration data directly from HMRC on your behalf. The data comes from HMRC, not from your network, so again no connection to your estate is required.

In both cases the flow is one-way and initiated outside your infrastructure. There is no scheduled job on your servers, no outbound feed to configure and nothing for your network team to permit beyond ordinary web access.

5 THE DATA WE HOLD

Every column of the production database has been catalogued in a field-level data inventory completed in June 2026. Each field is classified by personal data type, sensitivity, UK GDPR relevance, subject access and erasure relevance, protection applied and retention period.

DATA CATEGORY	WHAT IT COVERS	SENSITIVITY AND HANDLING
Customs declaration data	Import and export declaration records: commodity codes, values, quantities, duty and VAT amounts, procedure codes, origins and dates.	Commercial data, not personal data. Access restricted to named engineering staff on least privilege.
Trader identifiers	EORI numbers, and the names and addresses of declarants, importers and consignors appearing on declarations.	Business identity data that may constitute personal data for sole traders. Masking and access controls are prescribed by the inventory.
User account data	The name and business email address of each licensed user. This is the only data collected directly from individuals.	Business contact data. Passwords are never stored in readable form.
Special category data	None. No health, biometric, racial, political, religious or similar data is held.	NOT APPLICABLE Confirmed by field-level review, June 2026.
Payment card data	None. CAT360 does not take payments and never sees cardholder data.	NOT APPLICABLE PCI DSS is out of scope for this service.

6 WHERE YOUR DATA SITS AND WHO ELSE TOUCHES IT

Primary processing and storage is in the United Kingdom. The following are the only third parties involved in delivering the service.

SUBPROCESSOR	ROLE	LOCATION	CUSTOMER DATA INVOLVED
Amazon Web Services	Infrastructure hosting, storage and backup	eu-west-2, London, UK	Yes, all service data. AWS holds ISO 27001 and SOC 2 attestations.
SingleStore	Managed database service	Per data processing agreement	Yes, declaration and account data.
Sentry	Application error monitoring	Per data processing agreement	Minimal. Personal data scrubbing rules are enabled to keep customer data out of telemetry.
Vonage	SMS delivery	Per data processing agreement	Mobile number only, where SMS is used.
Google (Gemini)	Generates plain-English commodity descriptions	Per data processing agreement	None. It receives only publicly available UK HMRC Trade Tariff data.

Customer data is never sold, shared for any third party's own purposes, or reused in aggregated, anonymised or derived form. It is processed solely to deliver the contracted service.

7 SECURITY CONTROLS AT A GLANCE

The table below summarises the control position across the domains covered by a standard cloud vendor security assessment. A fully completed questionnaire with control-level detail and supporting evidence is available on request.

DOMAIN	STATUS	SUMMARY
Identity and access	IN PLACE	A formal Joiners, Movers, Leavers policy governs all platform access, with a role-to-access matrix, named approval, an access register and same-day revocation for leavers. Multi-factor authentication is enforced across our infrastructure and available to application users.
Privileged access	PARTIAL	Administrative access is through AWS Session Manager under IAM roles, with per-session audit records and no shared SSH credentials. Elevation is approved in advance and revoked within 24 hours. A dedicated privileged access management tool is not yet deployed.
Change and release management	IN PLACE	All changes pass through peer-reviewed pull requests with enforced branch protection and a gated pipeline covering static analysis, dependency vulnerability scanning and a full automated test suite. Releases are versioned and zero-downtime with a rehearsed one-step rollback.
Encryption	IN PLACE	All data in transit is encrypted with TLS. Secrets are held in AWS Parameter Store encrypted by AWS KMS, which uses FIPS 140-2

DOMAIN	STATUS	SUMMARY
		validated modules. Application-layer field encryption protects high-sensitivity personal data identified by the inventory.
Application security	IN PLACE	Static analysis and dependency scanning run on every change, with scheduled OWASP ZAP dynamic scanning against staging. An OWASP Top 10 assessment and STRIDE threat model form part of the development lifecycle. Output escaping and CSRF protection are enforced by the framework.
Network and system security	IN PLACE	Least-privilege, deny-by-default security groups expose only the ports the application requires. Production and staging are fully segregated, and the Barbourne Brook corporate network has no standing connectivity to production.
Logging and monitoring	PARTIAL	VPC flow logs, CloudWatch alarms, per-session administrative audit records, authentication logging and Sentry application monitoring with alert routing are all active. Dedicated SIEM and intrusion detection tooling is on the roadmap.
Risk management	IN PLACE	A live risk register carries every finding with a severity rating, named owner, ticket reference and committed remediation sprint. Closure requires recorded evidence and validation. The register originated from a full platform security audit in May 2026.
Physical security	INHERITED	Inherited from AWS data centres in London, which operate layered physical and electronic access controls evidenced by SOC 2 and ISO 27001 attestations. No Barbourne Brook employee or contractor has physical access to infrastructure holding customer data.
Training and personnel	IN PLACE	All staff complete annual data security, confidentiality, cyber security and GDPR training delivered through Hiscox. Confidentiality and data protection clauses are contained in all employment contracts. Policy violations must be reported within 24 hours.
Privacy and compliance	IN PLACE	Processing is conducted under UK GDPR, supported by the field-level personal data inventory, retention and erasure mapping, personal data scrubbing in telemetry and a published privacy policy. A data protection impact assessment has been carried out for HMRC-related processing.

8 AVAILABILITY, BACKUP AND RECOVERY

Backups	Automated daily volume snapshots under an AWS lifecycle policy with 60-day retention, plus managed database backups taken daily at 02:00 UK time with 7-day retention. No informal or ad hoc backups are used.
Recovery point	Worst-case data loss is under 24 hours. This meets a 48-hour recovery point objective comfortably.
Recovery time	A 24-hour recovery time objective is achievable. Application-level recovery is near-instant through the rehearsed rollback procedure, and full instance recovery from snapshots with automated redeployment sits well inside 24 hours.

Rollback testing	The application rollback procedure was rehearsed on staging in June 2026 and completed in under one second, with results documented. A database restore drill is scheduled.
Data residency on recovery	Backups remain within the same AWS region and provider boundary. Data does not leave the United Kingdom as part of any recovery process.

9 INCIDENT RESPONSE AND BREACH NOTIFICATION

Incidents are detected through Sentry application monitoring with alert routing and CloudWatch infrastructure alarms, both with established response paths. Every incident is categorised by severity and tracked in Jira with a named owner and a due date, and every security incident involving customer data receives a post-incident review against a standard template with remediation actions tracked to closure.

Our notification commitment. We will notify you of any security incident involving your data within 24 hours, through the account channels agreed in your contract. This sits alongside our own obligation under UK GDPR to report a qualifying personal data breach to the Information Commissioner's Office within 72 hours.

Forensic capability is supported by network flow logs, 60 days of point-in-time snapshots, per-session administrative access records and fully version-controlled releases, which together allow an incident to be reconstructed and evidence preserved. We will co-operate fully with any customer-led forensic investigation that is legally permissible.

10 CERTIFICATION AND COMPLIANCE POSITION

We would rather be straightforward about where we stand than let an assessment discover it later.

STANDARD OR REQUIREMENT	POSITION	DETAIL
Cyber Essentials Plus	CERTIFIED	Independently assessed and certified under the NCSC's Cyber Essentials Plus scheme. Certified 5 February 2026, valid to 5 February 2027, certificate reference 1c557d07-f00b-4c9e-bb7d-3dca354aa9b8. Verifiable by company name on the NCSC certificate search at iasme.co.uk.
UK GDPR and Data Protection Act 2018	COMPLIANT	Actively managed, supported by the field-level personal data inventory, retention and erasure mapping and a data protection impact assessment for HMRC-related processing. Our CAT360 Information Security Policy and Acceptable Use Policy are published at barbournebrook.co.uk.
Independent penetration test	COMPLETED	A full independent penetration test was completed in 2025 and the report is available under a non-disclosure agreement. The platform has since been rebuilt, and a retest of the rebuilt platform is scheduled.
Platform security audit	COMPLETED	A comprehensive security audit of the platform was completed in May 2026. Findings were severity-rated and have been substantially remediated through structured sprints, with evidence recorded at closure.
ISO 27001 and SOC 2	NOT HELD	Barbourne Brook does not currently hold either certification. The underlying infrastructure is covered by

STANDARD OR REQUIREMENT	POSITION	DETAIL
		AWS ISO 27001 and SOC 2 attestations, available through AWS Artifact.
PCI DSS	NOT APPLICABLE	The service does not receive, process, store or transmit cardholder data.
FedRAMP	NOT APPLICABLE	The service is not hosted in the United States and is not offered to US federal agencies.
Framework alignment	ALIGNED	Practices align to recognised frameworks: NIST 800-88 for media sanitisation, NIST 800-series least-privilege and zero-standing-credential principles, OWASP for application security and SLSA-aligned supply chain controls in the build pipeline.

11 WHAT WE ARE BUILDING NEXT

Our security programme runs on a continuous sprint cadence driven by the risk register. The items below are known gaps with a committed direction of travel, together with the controls that reduce the risk in the meantime.

ITEM	CURRENT POSITION	COMPENSATING CONTROL
Single sign-on and SAML	Not currently supported. Authentication is application-native. Prioritised subject to customer demand.	Passwords are salted and hashed with complexity rules and login rate limiting, and multi-factor authentication is available to users.
SIEM and intrusion detection	Dedicated tooling not yet deployed. On the security roadmap.	Network flow logs, infrastructure alarms, per-session administrative audit records and application anomaly monitoring are all active.
Managed endpoint control	Company devices are not yet under central mobile device management with remote wipe.	The service is browser-accessed and cloud-hosted, so customer data is not held on endpoints, and all production access is identity-based and centrally revocable.
Consolidated continuity plan	Recovery components are in place and rehearsed. A single document declaring recovery objectives per failure scenario is being finalised.	Rehearsed rollback, daily snapshots with 60-day retention, managed database backups and a documented recovery runbook.
Formal policy set	The CAT360 Information Security Policy and Acceptable Use Policy are published. The access control policy was issued June 2026 on a six-monthly review cycle. A service-specific data protection policy is in preparation.	Controls are implemented and evidenced in practice; the work is documentation of existing behaviour rather than new control design.
Annual assurance cycles	Annual access recertification, third-party review and continuity exercise cycles are defined and beginning their first full run.	Access is reviewed on every role change and at offboarding, and the risk register is reviewed at least weekly during active remediation.

12 AVAILABLE ON REQUEST

If your assessment process needs more than this summary, we can provide the following without delay. Please ask your Barbourne Brook contact rather than issuing a questionnaire, as it is usually faster.

Completed questionnaire	Our full cloud vendor security questionnaire response, covering more than 60 controls across 14 domains with a description of the programme and controls for each.
Penetration test report	The 2025 independent test report, under a non-disclosure agreement.
Data processing agreement	Our standard DPA, including the subprocessor schedule and transfer safeguards.
Access control policy	The Joiners, Movers, Leavers policy governing all access to the platform.
Personal data inventory	A summary of the field-level classification, including retention and erasure mapping.
Cloud provider attestations	Pointers to the current AWS ISO 27001 and SOC 2 reports covering the hosting environment.

WHO TO CONTACT

For security, data protection or contractual queries, please speak to your Barbourne Brook contact. They will route the question to the right person and can supply any of the material listed in section 12.

Barbourne Brook Ltd · barbournebrook.co.uk · CAT360 Information Security Policy: barbournebrook.co.uk/cat360-information-security-policy

About this document. Prepared by Barbourne Brook Ltd for organisations evaluating CAT360. It summarises our completed cloud vendor security questionnaire response, which covers more than 60 controls across 14 domains and is available in full on request. This document may be shared freely within your organisation and with your advisers. It is a summary and not a warranty; contractual commitments are those set out in the agreement between the parties.

Currency. Control positions, dates and roadmap items are accurate as at the issue date shown on page 1 and are subject to change as our security programme develops. Where a control is marked partial or planned, we are happy to discuss timing. If you are reading a copy more than six months old, ask us for the current version.