BUYER SECURITY SUMMARY

Security, privacy, and deployment

This brief separates controls that the current public website code supports from controls that must be designed and proved for a selected product deployment. Caracal does not claim a certification that is not complete and independently verifiable.

SCOPE	Public website baseline and pre-pilot deployment requirements. Product control evidence remains deployment-specific.

Architecture and controlled data flow

1	**Approved intake** The client and Caracal define the allowed supplier, site, route, item, system, or customer fields.
2	**Exposure model** The agreed data is structured into entities, relationships, dependencies, owners, and decision thresholds.
3	**External monitoring** Approved public and operational sources provide disruption evidence. Source links and timestamps remain visible.
4	**Decision output** The service prepares exposure-linked briefs, confidence, assumptions, uncertainty, and response options.
5	**Controlled handoff** Approved users receive dashboard, brief, alert, integration, or export outputs under the selected access rules.

Deployment models

HOSTED PILOT	DEDICATED VPC	ON PREMISE
A limited dataset and an agreed hosting region. Define access, retention, subprocessors, backups, and deletion before intake.	A client-specific cloud boundary. Design identity, networking, encryption, logging, backups, support access, and recovery with the client.	An option for high-sensitivity workloads. Agree update, support, monitoring, incident, and recovery responsibilities before use.

CONTROL REGISTER

Current status and buyer evidence

The status below is deliberately narrow. A deployment review must replace general requirements with named owners, tested settings, evidence, and contract terms.

CONTROL	STATUS	BUYER EVIDENCE
Transport security	Implemented for the production website	HTTPS redirect, HSTS, secure session and CSRF cookies, and production configuration.
Encryption at rest	Deployment requirement	Selected database, storage, backup, key-management, and secrets configuration.
Authentication and roles	Deployment requirement	Role matrix, identity-provider design, MFA decision, and authorization test results.
Audit logging	Website baseline; product evidence required	Sample events, access rules, retention period, and export method.
Retention and deletion	Defined per deployment	Data schedule, backup expiry, end-of-pilot deletion method, and verification record.
Tenant isolation	Architecture-dependent	Architecture diagram, authorization tests, storage boundaries, and support-access rules.
Backups and recovery	Deployment requirement	Frequency, encryption, retention, restore test, RPO, and RTO.
Vulnerability management	Website baseline; operating process required	Dependency review, scanning, patch targets, prioritization, and remediation records.
Incident response	Plan milestone	Plan owner, contact route, notification terms, and exercise record.
Subprocessors and residency	Disclose and agree before processing	Exact provider list, purpose, region, backup location, transfer path, and support access.

Data and model requirement

- Pilot and production terms must prohibit use of client data to train shared models by default.
- Any different use needs a separate written purpose, approval, data scope, retention rule, and deletion method.
- Outputs must distinguish confirmed facts, inferences, assumptions, and unknowns.

Before a pilot

- Agree the architecture, data flow, roles, region, retention, subprocessors, and recovery targets.
- Request test evidence for the controls used by the selected deployment.
- Use the security contact below for the deployment review.

SECURITY CONTACT info@caracalintelligence.com caracalintelligence.com/security/