VISTACRAFT

SECURITY REVIEW & INCIDENT RESPONSE

Engagement Authorisation

This form authorises ServeLogic Ltd, trading as Vistacraft ("the Provider"), to carry out the security review or incident response described below on the Customer's systems, which are hosted elsewhere and not on the Provider's infrastructure. No work starts until it is signed by both parties.

Identity verification is required. No work begins until your identity is verified through Stripe Identity, our third-party identity service. You will be sent a secure verification link at servelogic.co.uk/verify. I will not proceed with any work without a Stripe-verified pass.

Engagement reference: IR-[year]-[number], e.g. IR-2026-001 (this reference is also the name of the engagement's API key).

Service: ☐ Security review (authorised testing) ☐ Incident response / compromise recovery

Provider: ServeLogic Ltd (company no. SC873950), trading as Vistacraft. Contact: security@servelogic.co.uk, 07736 335135.

1. Customer and identity verification

The person signing must own the systems in scope, or be authorised to act for their owner.

Customer (person or organisation)	
Company number (if applicable)	
Signatory name	
Signatory role	
Email	
Phone	
Relationship to the systems	Owner / director / authorised representative

Identity verified by the Provider (completed before work starts):

Stripe Identity verification (session id and date)	
Ownership or control of the systems confirmed (e.g. domain registrant, hosting account holder)	
Verified by / date	

2. Authority to permit testing

Because the systems are hosted by a third party, the Customer confirms, before any work starts:

☐ The Customer owns the systems in scope, or is authorised by their owner to commission this work.

☐ The Customer's agreement with its hosting provider permits security testing of these systems, or the Customer has obtained the host's written permission. (Many hosts require advance notice for penetration testing.)

☐ The Customer will inform any third party whose systems or data could be affected.

3. Systems in scope

Only the systems listed here are covered. Anything not listed is out of scope, and the Provider will ask before going further.

System (domain, server, application or account)	Hosted where	Access the Provider will use

Explicitly out of scope: _____

4. Engagement dates

Work may only take place between these dates. Extending them needs a new signature or written confirmation from the signatory.

Start	
End	

5. Permitted activities

The Customer authorises the Provider, on the systems in scope and within the dates above, to:

- collect logs, file samples, configuration and code for analysis;
- examine the systems to identify vulnerabilities and, for incident response, how they were compromised and what was affected;
- for a security review, attempt to exploit identified vulnerabilities to demonstrate their impact, using the least intrusive method that proves the finding;
- develop a proof-of-concept and a safe reproducer for each confirmed finding;
- for incident response, contain a live compromise (blocking addresses, disabling accounts, taking a site offline briefly), remove malicious files and restore clean copies, and apply patches and hardening;
- verify that fixes work, without causing harm or disruption.

The Provider will not:

- access systems outside the scope above;
- carry out denial-of-service or load testing;
- exfiltrate, destroy or alter customer data beyond the minimum needed to prove a finding, using benign markers where possible;
- contact or act against third parties, including suspected attackers;
- make changes that could cause significant downtime without first agreeing a time with the Customer.

6. AI-assisted analysis and your data

The Provider uses AI tools from Anthropic (the Claude models) to help analyse evidence. Please read this before signing.

- Who uses it: only the Provider's director operates the AI tools. You never use them and receive only finished, reviewed work.
- What is shared: logs, file samples, configuration and code from the systems in scope, where needed. Passwords, keys and personal data are removed or masked wherever practical.
- How it is run: through the Provider's own Anthropic account, in a workspace ("vistacraft-ir") used only for this offering, with an access key issued for this engagement alone and revoked within one day.
- What you receive: see Deliverables. Raw AI output, transcripts and session logs are never handed over.
- Keeping and deleting data: evidence is kept only as long as the engagement and its follow-up need it, then deleted. You can ask for it to be deleted sooner.

☐ I consent to evidence from the systems in scope being analysed with AI tools as described above.

---

7. Deliverables

- Security review: a written, priority-ranked report of findings and recommended fixes; and, for each confirmed finding, a proof-of-concept and a safe reproducer that demonstrate it, so your developers can reproduce the issue and verify the fix. Plus any code changes agreed.
- Incident response: a written report covering how the systems were compromised, what was affected, what was cleaned or restored, and the hardening applied; plus any code or configuration changes.

Handling of proof-of-concept code:

- Proof-of-concept and reproducer code is provided to the Customer alone, for the Customer's own systems in scope, and must not be used against any other system or party.
- The Provider's working copies, including any weaponised version, are destroyed when the engagement closes.

---

8. Signatures

By signing, the Customer confirms they own the systems in scope or are authorised to approve this work and to permit testing of them, and the Provider confirms it will work only within the scope, dates and terms above.

	Customer	Provider
Name		Demis Cunningham
Role		Director, ServeLogic Ltd
Signature		
Date		

Vistacraft is a trading name of ServeLogic Ltd, registered in Scotland, company number SC873950.