Engagement Authorisation

Nov 17, 2026 · @Demis Cunningham

This form authorises ServeLogic Ltd, trading as Strathearn Hosting ("the Provider"), to carry out the compromise recovery or security audit described below on the Customer's systems. 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 (servelogic.co.uk/verify) or can enter your email there. The Provider will not proceed 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: ☐ Compromise recovery ☐ Security audit

Provider: ServeLogic Ltd (company no. SC873950), trading as Strathearn Hosting. 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.

Field	Details
Customer (person or organisation)	
Company number (if applicable)	
Signatory name	
Signatory role	
Email	
Phone	

Field	Details
Relationship to the systems	Owner / director / authorised representative

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

Check	Result
Method (e.g. video call against photo ID, existing hosting account holder, Companies House officer record)	
Ownership or control of the systems confirmed (e.g. domain registrant, hosting account, DNS change)	
Verified by / date	

2. 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: _____

3. Engagement dates

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

	Date
Start	
End	

4. 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 find how they were compromised and what was affected
- contain the compromise, for example by blocking addresses, disabling accounts or taking a site offline briefly
- remove malicious files and restore clean copies from backup where possible
- apply security patches and hardening changes
- test 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
- contact or act against third parties, including suspected attackers
- make changes that could cause significant downtime without first agreeing a time with the Customer

5. AI-assisted analysis and your data

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

- **Who uses it:** only the Provider's director operates the AI tools. You never use them yourself and receive only finished, reviewed work.
- **What is shared with it:** logs, file samples, configuration and code from the systems in scope, where needed for the analysis. Passwords, keys and personal data are removed or masked wherever practical before sharing.
- **How it is run:** through the Provider's own Anthropic account, in a workspace used only for customer engagements, with an access key issued for this engagement alone that expires within one day.
- **What you receive:** a written report and any code changes, reviewed by the Provider. Raw AI output, transcripts and session logs are never handed over.
- **Keeping and deleting data:** evidence collected for this engagement is kept only for 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.

6. Deliverables

- **Compromise recovery:** 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 made.
- **Security audit:** a written, priority-ranked report of findings and recommended fixes, plus any code changes agreed.

Reports describe weaknesses and how to fix them. They do not include working exploit code.

7. Signatures

By signing, the Customer confirms they own the systems in scope or are authorised to approve this work, 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		

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


ServeLogic