Security – Cloud, AI & Data Platforms

Service overview

We help public sector bodies secure services on AWS and Azure, including data platforms, web applications and AI. We set up identity and access management, review architecture for security, secure infrastructure as code, and put logging, monitoring and data protection in place. We help teams adopt generative AI safely, with clear controls on what AI tools can see and do. Our work follows NCSC Cloud Security Principles and GDS standards.

What is included

- Identity and access management (IAM, SSO, MFA)
- Secure architecture and design reviews
- AWS and Azure security configuration and hardening
- Security logging, monitoring and alerting
- Data protection for data platforms and web applications
- Safe and secure use of generative AI
- Secure infrastructure as code with Terraform
- Threat modelling and risk assessment
- Vulnerability management and remediation
- IT health check and Cyber Assessment Framework support

How we work

Stage	What happens
Assess	We review your architecture, access, configuration and risks against NCSC principles.
Plan	We agree a prioritised plan of fixes and controls with you.
Protect	We put controls in place: identity, encryption, logging, monitoring and AI guardrails.
Assure	We test, document and hand over, with evidence for audits and assessments.

What you get

- Security review with risks ranked by severity
- Threat model
- Identity and access design

- Logging, monitoring and alerting set-up
- Controls and guardrails for AI tools
- Evidence pack for Cyber Assessment Framework, IT health checks and audits

What is not included

- Risk acceptance and accreditation decisions, which stay with your organisation
- Physical security of your premises
- 24/7 security operations centre monitoring, unless agreed

Examples of our work

Cabinet Office Digital – GRID. GRID holds sensitive workforce data from many departments. We built in attribute-based access controls, anonymisation and DevSecOps practices aligned to Cabinet Office data governance standards, so approved users see only the data they should.

Intelligence and Security Committee of Parliament. We supported and improved the committee's WordPress service and moved it to a simpler, lower-cost AWS Lightsail set-up (2024 to 2025), without disruption. Given the committee's remit, reliability and security were critical. We met 100% of SLAs, with no service issues.

About Four Seals Digital

Four Seals Digital Limited is a UK digital agency that works with the public sector. Our team of around 25 people includes solution architects, engineers, data analysts, AI engineers, business analysts, and product and delivery managers.

We have long experience of working with UK central government. We build and support web applications, data platforms and AI services on AWS and Azure.

We are certified to ISO 27001. All our staff and operations are in the UK, and we have staff with Security Check (SC) clearance.

Standards we follow

- GDS Service Standard and Technology Code of Practice
- NCSC Cloud Security Principles and Cyber Assessment Framework
- ISO 27001 information security management
- UK GDPR and the Data Protection Act 2018
- WCAG 2.2 AA for anything users see

Security and your data

We work inside your own cloud accounts wherever possible, and ask for the least access we need (read-only where that is enough). Your data stays in the UK and is handled only by UK-based staff. We do not share your data with anyone else, and we return or securely delete it when the work ends.

Starting the service

- Kick-off meeting to confirm goals, scope, contacts and ways of working
- Agree access, security clearance needs and any data sharing terms
- Agree service levels, reporting and how we raise and escalate issues
- Short discovery to confirm the plan before main delivery starts

Ending the service

- Hand over all code, documents, dashboards and configuration
- Knowledge transfer sessions with your team or new supplier
- Return or securely delete your data, and confirm this in writing
- Remove our access to your systems and accounts

Support and service levels

We offer working-hours support (9am to 5pm), extended support on working days, or 24 hours a day, 7 days a week. We agree the right level with you. Typical response times are below; resolution targets are agreed in the order.

Severity	What it means	We respond
Service down	A core service is unavailable	Immediately
Critical	Business outage or major impact on users	Within 1 hour
Urgent	Service works but is badly affected, or a time-sensitive issue	Within 2 hours
Important	Issue with little current impact on users	Within 4 hours
Monitor	No action needed beyond monitoring	Within 1 working day
Information	Request for information only	Within 1 working day

Who does what

You will:

- Give us access to the systems, data and people we need
- Name the people who can raise and approve requests
- Raise issues through the agreed route and set their priority

We will:

- Deliver the agreed work to the agreed standards

- Track every issue through to resolution and keep you updated
- Escalate problems early, through the agreed route

Contact us

Four Seals Digital Limited, Office 2, Tweed House, Park Lane, Swanley, BR8 8DT. Contact us through the Digital Marketplace to discuss your needs.