Sentinel by SCC – secure public sector cloud

You hold public sector data – Sentinel protects it.

The trusted way to deploy your IT

Sentinel was the first Pan-Government Accredited public sector cloud, operating to CESG IL2 and IL3 (now OFFICIAL / OFFICIAL Sensitive) security standards.

Accredited

The entire platform, inclusive of hardware, software and network, is pan-government accredited for a multi-tenanted environment and we are an accredited PSN service provider (PSNSP).

This means that the environment:
• Offers a re-usable accreditation ensuring that a customer’s own internal security approvals process is significantly reduced
• Greatly reduces risk
• Ensures full compliance and assurance of the service according to the code of connections mandated by the PSN Authority for PSNSPs

Quality

Quality and continuous improvement are integral to our business strategy and we continually improve our processes, systems, procedures and people. Our services are underpinned by certification for process and procedures (ISO 9001), environment (ISO 14001), security (ISO27001), ITIL (ISO 20000), and health and safety (OHSAS 18001).

Managed

The tenancy can be fully managed, reducing the burden on your organisation’s own internal IT staff, meaning that any failures are handled appropriately and in accordance with agreed procedures. This leaves a customer’s own IT teams to concentrate on their core services and not worry about the underpinning infrastructure.

UK Sovereignty

SCC has Tier 3+ UK data centres and therefore is not subject to Off Shoring or Near Shoring restrictions.

Network Operation Centre (NOC)

This allows us to provide, configure, manage and maintain a new environment or provide cost-effective enhancements for an existing solution.

Security Operation Centre (SOC)

This is where we monitor, assess and protect customers’ enterprise information systems.

Owned Infrastructure

The infrastructure is SCC owned, utilising internal security cleared resources, meaning that as Prime Contractor we are accountable for the contract and not reliant on 3rd parties.

Network Connectivity

SCC ensures the ability to connect with the Sentinel platform via encrypted internet, the PSN, N3 and PNN Government Networks.

24x7 Support

SCC-employed, UK-based, SC-cleared cloud engineers available 24 hours a day, 7 days a week.

ITIL Aligned Service

SCC’s Service Management tools and service are fully aligned to ITIL and are certified to ISO 20000 – including Incident, Change and Problem Management.

Sentinel by SCC offers

• Price predictability – you can pay as you go
• Guaranteed SLAs – ensuring 99.9% or 99.95% availability
• Service, not just servers – our solution is fully managed 24x7
Infrastructure-as-a-Service (IaaS)

Bronze
Our rawest infrastructure service connected to the internet and ideal for development or proof of concept exercises. We provide the hypervisor, you do the rest.

Silver
A flexible and secure infrastructure service connected to government bearers (PSN), with options for SLAs. A customisable menu of services allowing customers to pick and choose what they’d like to retain in-house for application or operating system control.

Gold
A fully managed and monitored secure infrastructure service connected to government bearers (PSN) with options for SLAs. Provides full monitoring, alerting and OS support.

Sentinel by SCC’s IaaS options include:

Storage
SCC’s Secure Storage service provides readily available, managed scalable storage up to OFFICIAL of the Government Security Classification Policy. Inclusive within this is caveated information, such as OFFICIAL Sensitive.

Backup
SCC’s Secure Backup service provides secure, readily available, ready-to-run managed backup of your environment.

Software-as-a-Service (SaaS)

Exchange as a Service (EaaS)
Sentinel hosted Exchange is a business class messaging service, providing not only your OFFICIAL hosted email but also allowing you to share calendars and book meeting rooms.

Skype for Business
Skype for Business delivers an end-to-end OFFICIAL hosted unified communications solution, while giving staff a consistent experience for presence, IM, HD voice and HD video across PCs, Macs, phones and tablets.

Mobility as a Service (MaaS)
Our mobility service enables flexible access to OFFICIAL environments allowing mobile application deployment and management with options for synchronised email, calendar, contacts and restricted internet on your device in accordance with UK government end user device guidance.

Managed Desktop Services
Sentinel OFFICIAL Managed Desktop Services for end point management allows you or SCC to support either a Windows or Apple-based experience for your end users, aligned to UK government end user device guidance.

Hosted Desktop as a Service (HDaaS)
Sentinel OFFICIAL Hosted Desktop delivers standardised corporate desktop and MS Office software on a simple per user, per month payment model as a fully managed solution with 24/7 support.

Remote Access as a Service (RAS)
The SCC Secure Remote Access Service provides a robust and secure mechanism to access OFFICIAL environments from an internet connection in accordance with UK government end user device guidance.

Database as a Service (DBaaS)
SCC Database as a Service (DBaaS) leverages the efficiencies of the cloud to provide a comprehensive solution for organisations wanting to remove the resource overhead of deploying and managing an OFFICIAL database environment.

Secure File Sharing and Collaboration
Enables organisations to securely connect mobile workers with enterprise content across any device within an OFFICIAL environment and in accordance with UK government end user device guidance.

Service Management
Sentinel by SCC’s IaaS will be operated and managed securely in order to detect, impede or prevent attacks against it. It has options for ITIL aligned service management, disaster recovery and service desk functions including:

Configuration and change management – ensuring that changes to the system do not unexpectedly alter security properties and have been properly tested and authorised.

Protective monitoring – taking measures to detect attacks and unauthorised activity on the service

Incident management – ensuring the service can respond to incidents and recover a secure available service.

We take the responsibility for these elements to ensure that you can be confident the service remains assured and compliant with the current security guidance.