Infrastructure as a Service (IaaS)
Compute with Secure Storage and Secure Backup
1 Introduction to Infrastructure as a Service

Using an Infrastructure as a Service (IaaS) will allow Customers to rapidly add or remove capacity, with billing against resource usage. This provides a great deal of flexibility and the ability to hold costs down. It is ideally suited for services with cyclical or seasonal peaks or those with uncertain demand. Sentinel, by SCC, not only provides faster IT implementation but also keeps data secure to CESG security standards (including OFFICIAL). It is an established and cost-effective Cloud solution and was the first to be Pan-Government Accredited. Sentinel removes contract lock-ins, simplifies integration, shortens development times, reduces waste and most importantly, lowers cost. It facilitates rapid deployment of on-demand services and the scaling of IT resources. The platform offers Public Sector bodies the ability to share the cost of infrastructure between multiple organisations, whilst taking advantage of latest technologies, best practice solutions and economies of scale.

Highlights

The Sentinel Infrastructure as a Service offering includes the following:

- A fully accredited, Network, Compute and Storage Platform
- Secure Government “Community Cloud” Offering
- Pay as you go compute model
- Flexible environments
- Number of pre-sized machine offerings available
- Incremental, customised sizing options available upon request
- Multiple Operating Systems supported
- Three pre-defined service models available for environments providing varying levels of Service Management and Support - Bronze, Silver and Gold
- GPG 13 Compliant (DETER) platform
- Ability to connect to the Sentinel platform via the Internet, the GCF and the PSN Government Networks
- Guest level back up each evening, with a standard 14 day retention period (limited to the boot partition) included
- Single and dual site options provide two levels of compute availability
- Built upon industry standard components and services
- Option for Deployed Physical Asset (Hybrid Cloud)
2 Service Definition

2.1 Compute

Step one: Customers select their virtual infrastructure requirements. Using the table below, select Mini, Small, Medium or Large virtual machines and the quantities of each size. Customers also need to decide on whether they require single or dual site for their infrastructure components. It is possible to mix and match within a single infrastructure. For example, web servers can be single site but the application servers can be dual site and the virtual machine images replicated to the secondary data centre for disaster recovery. Additionally, customers can select any RAM or vCPU increments if required over and above the pre-sized templates.

2.1.1 Compute – Infrastructure

There are 4 standard infrastructure size variations available within SCC’s Sentinel IaaS offering. These are as follows:

<table>
<thead>
<tr>
<th></th>
<th>Memory (GB RAM)</th>
<th>Number of vCPU’s</th>
<th>Storage Boot Partition Size (GB)</th>
<th>Storage PageFile (GB)</th>
<th>Single Site Price</th>
<th>Dual Site Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mini</td>
<td>2</td>
<td>1</td>
<td>90</td>
<td>10</td>
<td>£84.00</td>
<td>£178.00</td>
</tr>
<tr>
<td>Small</td>
<td>4</td>
<td>1</td>
<td>90</td>
<td>10</td>
<td>£107.00</td>
<td>£217.00</td>
</tr>
<tr>
<td>Medium</td>
<td>8</td>
<td>2</td>
<td>90</td>
<td>10</td>
<td>£196.00</td>
<td>£393.00</td>
</tr>
<tr>
<td>Large</td>
<td>16</td>
<td>4</td>
<td>90</td>
<td>10</td>
<td>£375.00</td>
<td>£747.00</td>
</tr>
</tbody>
</table>

*1 x vCPU = up to 2 GHz

If customers wish to expand resources over the pre-set virtual machine sizes in the table above, SCC offer the option to expand RAM and add vCPUs. The options available for expanding the standard infrastructure offerings are as follows:

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Single Site</th>
<th>Dual Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GB RAM increment</td>
<td>£12.00</td>
<td>£21.00</td>
</tr>
<tr>
<td>vCPU Increment</td>
<td>£59.00</td>
<td>£111.00</td>
</tr>
</tbody>
</table>

SCC’s Sentinel platform is housed within Tier 3+ Datacentres and provides resiliency at all levels of the infrastructure, providing a stable, reliable infrastructure platform. In order to provide additional levels of availability and redundancy, SCC provide the option for a dual site implementation, utilising SCC’s secondary Data Centre as a cold standby facility for the customer’s infrastructure. The following table provides the options available for Single site and Dual Site Infrastructure options and the corresponding Availability Service Level Agreement:

<table>
<thead>
<tr>
<th>Infrastructures Option</th>
<th>Availability SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Site</td>
<td>99.9%</td>
</tr>
<tr>
<td>Dual Site</td>
<td>99.95%</td>
</tr>
</tbody>
</table>
2.1.2 Compute – Service

Step two: Customers select their service level requirements for the virtual infrastructure within their cloud tenancy. SCC are uniquely placed to offer a complete mix and match provision within a cloud tenancy. For example, customers can select web servers on a Gold Service and then, due to application compatibility, select application servers on a Silver Service with Anti-virus and OS Monitoring as optional extras.

SCC’s Sentinel platform provides three standard service models as part of its IaaS offering. Each of these Service Models aims to meet the different needs of its customers by providing varying levels of integration and support. The three options are as follows:

1. **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. Please refer to the table below for a full breakdown of services that are in and out of scope:

2. **SILVER** – A flexible and secure infrastructure service connected to government bearers (PSN), with options for SLA’s. 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. Please refer to the table below for a full breakdown of services that are in and out of scope:

3. **GOLD** - A fully managed and monitored secure Infrastructure service connected to government bearers (PSN) with options for SLA’s. Provides full monitoring, alerting, ITIL aligned Service Management, Disaster Recovery and Service Desk functions. Please refer to the table below for a full breakdown of services that are in and out of scope:

<table>
<thead>
<tr>
<th>Service Cost</th>
<th>BRONZE</th>
<th>SILVER</th>
<th>GOLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>£0.00</td>
<td>£59.00</td>
<td>£136.00</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Options</th>
<th>BRONZE</th>
<th>SILVER</th>
<th>GOLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute Availability</td>
<td>99.90%</td>
<td>99.90% &amp; 99.95%</td>
<td>99.90% &amp; 99.95%</td>
</tr>
<tr>
<td>GSC</td>
<td>OFFICIAL</td>
<td>OFFICIAL</td>
<td>OFFICIAL</td>
</tr>
<tr>
<td>Connectivity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSN Assured</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSN Protected (GCF/Encrypted Overlay)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PSN IPED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site to Site VPN N3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Orchestration Portal</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Monitoring Portal</td>
<td>£3 per month per VM</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DR Option (99.95%)</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Available OS</td>
<td>Any supported by vSphere 5¹</td>
<td>Any supported by vSphere 5¹ and 2</td>
<td>Any supported by vSphere 5¹ and 2</td>
</tr>
<tr>
<td>OS Support</td>
<td>✗</td>
<td>£63 per month per VM</td>
<td>✓</td>
</tr>
<tr>
<td>OS Patching</td>
<td>✗</td>
<td>£26 per month per VM</td>
<td>✓</td>
</tr>
</tbody>
</table>
OS Monitoring | ✗ | £16 per month per VM | ✔
Antivirus | ✗ | £3 per month per VM | ✔
GPG13 | ✗ | £7 per month per VM | ✔
NTP Service | ✔ | ✔ | ✔

Optional step three: A customer may wish to ‘add on’ additional service options to each server according to its function. The relevant figures for optional ‘add on’ services are detailed below and can then be added to the cost illustration.

<table>
<thead>
<tr>
<th>Add-Ons</th>
<th>BRONZE</th>
<th>SILVER</th>
<th>GOLD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Repository</td>
<td>✗</td>
<td>£3 per month per VM RHEL 5 &amp; 6, Win 2003, Win 2008, Win 2012, CentOS 6</td>
<td>N/A</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>✗</td>
<td>£60 per change request</td>
<td>£60 per change request</td>
</tr>
<tr>
<td>Forward Proxy</td>
<td>✗</td>
<td>£1.95 per user/device per month</td>
<td>£1.95 per user/device per month</td>
</tr>
<tr>
<td>Reverse Proxy</td>
<td>✗</td>
<td>£30 per published URL per month</td>
<td>£30 per published URL per month</td>
</tr>
<tr>
<td>Application Monitoring</td>
<td>✗</td>
<td>£14 per month per application instance</td>
<td>£14 per month per application instance</td>
</tr>
<tr>
<td>Hybrid Cloud*</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>DR Testing</td>
<td>✗</td>
<td>£POA</td>
<td>£POA</td>
</tr>
<tr>
<td>ITIL Support</td>
<td>✗</td>
<td>£POA</td>
<td>£POA</td>
</tr>
</tbody>
</table>

*NB - SCC are also able to provide a Cloud Service encompassing physical and virtual servers to Sentinel tenants. Utilising our network links we are able to provide the capability for cloud tenants to deploy a mixed estate as part of their migration to the cloud. This allows organisations and departments to manage resources in-house and have some resources deployed and managed via SCC’s Sentinel cloud platform. The customer must incorporate their hybrid requirement alongside a Sentinel based tenancy.

2. Also RHEL5 & RHEL6

2.1.2.1 Compute – Hybrid Cloud

Optional step four: If customers require the deployment of a hybrid cloud – e.g. resources residing in Sentinel and resources that cannot be virtualised, maybe due to licence constraints – then customers can select the relevant option from the table below and apply the pricing to the overall cost illustration. Customers can then select individual service features listed under the ‘Silver’ option in the table detailed in Section 2.1.2.
2.2 Secure Storage

Step five: Customers select their storage requirements within the cloud tenancy. Customers have the flexibility of mixing and matching storage tiers related to the workloads. A purchased set of storage can be split across several virtual machines – not just associated to one. For example, a 20GB Tier 2 disk can be split across two web servers and two application servers – 4 x 5GB or any permutation there-of.

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:

- On a per GB per month basis
- Scalable up or down
- Comprising 3 tiered options
  - Tier 1 – High Performance transactional database and VDI
  - Tier 2 – Mid Level performance for standard applications
  - Tier 3 – Archival purposes
- With a choice of 99.9% and 99.95% availability delivered from single or dual UK data centres depending upon the SLA required
- With backup from our Secure Backup Service available as an additional service
- The service will be billed monthly in arrears
- The pricing for this service shall be based upon the units of storage consumed with a variance made for the availability service level required:

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Unit Cost Per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Managed Storage (Single Site)- Tier 1</td>
<td>£0.23 per GB</td>
</tr>
<tr>
<td>Secure Managed Storage (Single Site)- Tier 2</td>
<td>£0.17 per GB</td>
</tr>
<tr>
<td>Secure Managed Storage (Single Site)- Tier 3</td>
<td>£0.05 per GB</td>
</tr>
<tr>
<td>Secure Managed Storage (inc Replication)- Tier 1</td>
<td>£0.47 per GB</td>
</tr>
<tr>
<td>Secure Managed Storage (inc Replication)- Tier 2</td>
<td>£0.33 per GB</td>
</tr>
<tr>
<td>Secure Managed Storage (inc Replication)- Tier 3</td>
<td>£0.10 per GB</td>
</tr>
</tbody>
</table>
2.3 Secure Backup

**Step six:** Customer selects the required Backup Service; Basic, Standard or Enhanced. The table below details the service specifics with retention details and customers have the option to have backup data replicated to the secondary SCC data centre.

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

- On a per GB per month basis
- With a choice of 99.9% and 99.95% availability delivered from single or dual UK data centres depending upon the SLA required
- Connected to the secure backup network
- Image level backups with agent based restore
- Application aware backups. Examples include: Exchange, SQL, SharePoint, and Active Directory

The pricing for this service shall be based upon the units of backup consumed by the service with a variance made for the availability service level required.

The base unit costs for the service shall be offered against the following performance metrics:

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Single Site Unit Cost Per Month</th>
<th>Dual Site Unit Cost Per Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Secure Backup - Backup to disk (7 Days Retention)</td>
<td>£0.50 per GB</td>
<td>£0.65 per GB</td>
</tr>
<tr>
<td>Standard Secure Backup - Backup to disk (14 Days Retention)</td>
<td>£0.55 per GB</td>
<td>£0.75 per GB</td>
</tr>
<tr>
<td>Enhanced Secure Backup - Backup to disk (30 Days Retention)</td>
<td>£0.65 per GB</td>
<td>£0.85 per GB</td>
</tr>
<tr>
<td>Over 30 Days Off-site Tape</td>
<td>£POA</td>
<td>£POA</td>
</tr>
<tr>
<td>Price includes 6 restores per annum</td>
<td>£60 per additional restore</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- Backup Elasticity – As required relative to the capacity allocated on the primary Storage as a Service platform
- The service shall then be billed per unit per month in arrears
- The agents necessary to backup specific products will be required and defined within the initiation of the service with the Customer
2.4 Networking

Step seven: The final step is to determine the network requirements. As per the table in Section 2.1.2, SCC are able to provide differing connectivity options.

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Notes</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>Connectivity to the internet on dedicated bandwidth</td>
<td>£23 per Mb/s</td>
</tr>
<tr>
<td>PSN Assured Connectivity</td>
<td>Connectivity to the PSN on dedicated bandwidth</td>
<td>£20 per Mb/s</td>
</tr>
<tr>
<td>PSN Protected Connectivity</td>
<td>Connectivity to PSN Protected on dedicated bandwidth</td>
<td>£40 per Mb/s</td>
</tr>
<tr>
<td>Secure Internet Gateway</td>
<td>For secure internet browsing including: web filtering, reporting and monitoring</td>
<td>£245 per month</td>
</tr>
</tbody>
</table>
| SCC site to site VPN        | Connectivity to Sentinel via a SCC managed encryption service using CPA Foundation Grade devices | One-Off Set Up £4,500.00  
                              |                                                                      | Monthly Recurring - £1,250.00 |
| N3 Connectivity             |                                                                      | £POA                 |
| Internet Facing Denial of Service Protection | Denial of Service protection for internet facing web sites and services | £POA                 |

As part of the sales engagement, SCC will work with the customer to understand their cloud requirements and walk them through the process from virtual infrastructure through to the connectivity requirements and appropriate solutions. Customers are also invited to email gcloud@scc.com for a copy of our cost calculator to help with your journey to the cloud.

Alternatively, you can use the email address to contact us for access to highly skilled pre-sales and delivery experts.
3 Differentiators

SCC was the first pan-Government accredited provider of a G-Cloud platform. We have experience and capability across all cloud types (private, hybrid, community and public), combined with Information Assurance services that will help support PSN compliance. Potential customers can be assured that our maturity in providing Cloud based services differentiates SCC from a number of other IaaS cloud providers within the Digital Marketplace. Some differentiators include:

- **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 PSNSP’s.

- **Security Practice** – SCC utilises its own Information Assurance Practice to support the delivery of IT solutions into the government marketplace. We have found this internal function to be hugely beneficial to customers in the end to end IA design through to accreditation sign off; the IA practice, although internal to SCC, is independent to the operation of the platform, as such, supports the separation of duties principle without being 3rd parties for this additional critical service

- **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 (14001), security (27001), ITIL (20000), and health and safety (OHSAS 18001)

- **Managed** – the tenancy can be fully managed, reducing the burden on your organisations own internal IT staff meaning that the uptime availability provision is leveraged to ensure 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** – UK Data Centres and therefore not subject to Off Shoring or Near Shoring restrictions

- **Network Operation Centre (NOC)** – Allows us to provide, configure, manage and maintain a new environment or provide cost effective enhancements for an existing solution

- **Security Operation Centre (SOC)** – Where we monitor, assess and protect customers enterprise information systems

- **Owned Infrastructure** – 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** – Ability to connect to the Sentinel platform via the Internet, the GCF and the PSN Government Networks

- **24x7 Support** – SCC employed UK based, SC cleared, Cloud engineers available 24x7

- **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
4 Information Assurance

Sentinel has achieved both Pan Government Accreditation (PGA) and PSN Accreditation for systems at OFFICIAL. The service has also been implemented with the following security features:

- Suitable for OFFICIAL assets under the GSC (Government Security Classifications Policy)
- PGA accredited Inter-Domain Gateway – designed to facilitate assured connectivity between higher security domains and lower security domains or for organisations that wish to move more sensitive data assets at OFFICIAL
- SCC also holds ISO9000, ISO14001, ISO20000 and ISO27001 certifications which underpin our business operations and Cloud Platform
- All datacentres are highly resilient Tier3+, and UK based
- SCC is a registered sponsor with the Defence Business Services National Security Vetting (DBS NSV) which enables us to sponsor and administer the applications of Security Check (SC) and also Developed Vetting (DV) with the appropriate sponsorship from a customer
- As a minimum, all staff are cleared to Baseline Personnel Security Standard (BPSS)
- In excess of 800 staff are Security Cleared and based in the UK
- Protective Monitoring (aligned with GPG13 - DETER) across all Sentinel platforms at the hypervisor layer and below
5 Service Levels

The Services shall be provided by SCC in accordance with the following Service Levels;

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Availability (Single Site)</td>
<td>99.9%</td>
<td>99.9%</td>
<td>99.9%</td>
</tr>
<tr>
<td>Service Availability (Dual Site)</td>
<td>N/A</td>
<td>99.95%</td>
<td>99.95%</td>
</tr>
<tr>
<td>Hours of Service Desk Support</td>
<td>9 – 5</td>
<td>24 Hours</td>
<td>24 Hours</td>
</tr>
<tr>
<td>Incident and Problem Management Levels</td>
<td>4</td>
<td>1 - 4</td>
<td>1 - 4</td>
</tr>
</tbody>
</table>

The following tables provide a maximum time before a response to an incident is provided by Incident Management:

<table>
<thead>
<tr>
<th>Priority-(Severity)</th>
<th>Target Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - (Critical)</td>
<td>30 mins</td>
</tr>
<tr>
<td>2 - (High)</td>
<td>60 mins</td>
</tr>
<tr>
<td>3 – (Medium)</td>
<td>4 Hours</td>
</tr>
<tr>
<td>4 - (Low)</td>
<td>72 Hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Service Level</th>
<th>Incident Resolution Target</th>
<th>Hours of Support</th>
<th>SLA Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Managed Storage (Single Site)</td>
<td>Service Availability</td>
<td>4 Hours</td>
<td>24 Hours</td>
<td>99.9%</td>
</tr>
<tr>
<td>Secure Managed Storage (Failover Site)</td>
<td>Service Availability</td>
<td>4 Hours</td>
<td>24 Hours</td>
<td>99.95%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Component</th>
<th>Service Level</th>
<th>Incident Resolution Target</th>
<th>Hours of Support</th>
<th>SLA Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Backup (Single Site)</td>
<td>Service Availability</td>
<td>4 Hours</td>
<td>24 Hours</td>
<td>99.9%</td>
</tr>
<tr>
<td>Secure Backup (Failover Site)</td>
<td>Service Availability</td>
<td>4 Hours</td>
<td>24 Hours</td>
<td>99.95%</td>
</tr>
<tr>
<td>Secure Backup</td>
<td>Service Request (Controlled &amp; Managed by SCC)</td>
<td>Next business day</td>
<td>8am to 6pm</td>
<td>99.5%</td>
</tr>
<tr>
<td>Priority (Severity)</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| **1 - (Critical)** | An incident which involves service not available or a serious malfunction of the service with impact on Sentinel’s direct delivery to single or multiple customers  
  - Total loss of service to all users and no work-around available  
  - Loss of functionality resulting in Sentinel Customer users/workgroups being unable to continue with normal business processing  
  - Unavailability of one or more supported services  
  - Sentinel down |
| **2 - (High)**    | An incident which involves service not available with impact on Sentinel’s single or multiple customers or a serious malfunction of the service with potential impact on Sentinel’s direct delivery to customers  
  Partial loss of service and work-around available  
  - Loss of functionality which severely impedes all or some Sentinel services  
  - Customers’ users/workgroups being able to continue with normal business processing  
  - Partial loss of availability of one or more supported service |
| **3 – (Medium)**  | An incident that involves degradation or risk to quality of service with impact on one or more Sentinel customers  
  - Issue not impeding Sentinel customers’ users/workgroups from being able to continue with normal business processing  
  - Potential to cause more serious issue if not investigated and addressed |
| **4 - (Low)**     | An incident for which the final resolution is outside the control of Sentinel and Sentinel has used all reasonable endeavours to mitigate the impact of the incident to the Customer. Sentinel shall advise the Customer of the likely resolution date and shall notify progress against this date.  
  General Service related questions and requests for information. |
6 Backup/Restore and Disaster Recovery

For the Basic, Standard and Enhanced Service offerings, the Virtual Machines shall be backed up to disk each day and backups will be retained for 14 days as standard with 7 or 30 day options, depending on the core service offering selected.

This backup shall be limited to the standard boot partition of the virtual machine and will not include additional persistent (Data) storage connected to the service.

Backup of additional “Application” data is provided under SCC’s Secure Backup Service available under GCloud.

Backup will be to disk only. Backup of the OS to tape is offered as an additional, separate service.

Recovery of a VM Image from backup shall be actioned within 4 Hours from the point of request by The Customer through the SCC Service Desk. The time taken to recover a Virtual Machine will be dependent upon the size and the complexity of the restore process for the specific machine.

Additional levels of backup service can be provided as part of the Secure Backup Service offering.

Where a customer has selected the 99.95%, higher availability service, the VM Image shall be replicated in real time to a secondary data centre. Compute resource shall also be allocated at the secondary site, providing a cold standby “Disaster Recovery” solution. In the eventuality that the primary site fails, and a Disaster is declared, the service shall be restored at the secondary datacentre.
7 Additional Information

7.1 Technical Requirements - Service Dependencies

7.1.1 Compute

The Customer will require network connectivity either via the Internet or via a Government Network in order to access the Sentinel platform.

The Customer will be responsible for ensuring they meet the requirements of the associated Code of Connections.

A migration on to the Sentinel platform will be possible once necessary due diligence and infrastructure sizing exercises have been undertaken. These exercises can be undertaken via SCC as part of a professional services engagement.

As part of any migration on to the Sentinel service, the Customer would be responsible for the following activities:

- Where existing Virtual infrastructure is being migrated, where appropriate, provide SCC with a VMDK or OVF Image and/or license keys and any other information reasonably required to enable the initial server build
- In the event the Customer wishes to implement any operating systems software which is not identified on the SCC supported operating system software list, then prior to such implementation the Customer must first agree such with SCC
- Procurement, maintenance and management of any data communications lines not identified in the Order Form and/or Agreement
- Provision, maintenance and management, of any Customer software, operating systems, applications and data which resides on the Sentinel Infrastructure which is not within the scope of the Agreement
- Administration, management and control of Users access to the Customers applications and/or data stored on the Sentinel Infrastructure
- Should SCC determine that the Customers usage of the Sentinel Infrastructure is not compliant with best practice guidelines then the Customer must comply with SCC’s reasonable requests for change

In the event that the Customer requires the implementation of its own anti-virus software, then this will be by mutual agreement with SCC.

7.1.2 Secure Storage

This service shall deliver a Secure Storage platform. SCC shall provide tiered disk, within a fully monitored and managed SAN environment.

Customer data shall be loaded on to the secure storage service in conjunction with SCC accredited and security cleared staff, who shall be responsible for all in-scope on-boarding tasks associated with the delivery of this service.

The secure storage service will be managed by SCC security cleared staff, including:
• Availability of the Storage Service Infrastructure
• Capacity utilisation of the Storage Service being used

Requests for additional storage requirements shall be made, either via the service desk or the service request process.

The Customer will be responsible for ensuring adequate bandwidth is provided for their user community to effectively access the data residing within the Secure Storage Service, within the SCC Sentinel platform. This would be agreed and implemented at the initiation of the contract and managed through service change management process from that point. If the connecting bandwidth is supplied through SCC’s Sentinel platform then this will be capacity managed by SCC and reported to the Customer.

7.1.3 Secure Backup

This service delivers a Secure Backup as a Service platform. SCC shall provide a secondary backup and optional tape library platform appropriate to the backing up of the Customers data needs, within a fully monitored and managed environment.

Customer data shall be backed up to the primary secure storage service.

The secure backup service shall be fully managed by SCC security cleared staff, including:

• Availability of the Backup Service Infrastructure
• Measuring the Backup Service capacity being used

Requests for additional backup capacity shall be made, either via the service desk or the service request process.

Customer to provide Data Governance policy for the backup, restore and data retention, incorporating policies for possible media handling, where required.

Optional tape retention and rotation will be agreed at contract initiation.

7.2 Service Constraints

The service shall be allocated a maintenance window between the hours of 23:00 and 06:00 and the window shall be allocated during service initiation.

The service shall be Change Managed in accordance with SCC change schedules. Change boards will sit weekly and changes shall be carried out during subsequent change window.

Configuration changes that cause a reboot/downtime but are deemed urgent shall not impact Availability metrics, SLAs and the associated charging mechanism.

SCC will not provide any application or middleware level support as part of the service offerings described within this agreement.

The ability to add move or change the number of VMs in the Customer solution shall be achieved via the Service Request process and may be subject to appropriate financial approvals.

VMs shall be decommissioned via change control and images will be shut down. The images will be left in place for a further 24 hours after which point they will be deleted.
As part of any decommissioning process all virtual backups will be destroyed and any physical backups will be returned to the Customer or destroyed.

Decommissioned machines shall be quarantined and can be restored to full operational state within 24 hours of being decommissioned.

Customers will also have the ability to add, move or change the storage capacity in The Customer solution via the Service Request process, subject to financial approvals. Configuration changes that cause a reboot/downtime but are deemed urgent shall not impact SLAs and the associated charging mechanism.

The Customers will also have the ability to add move or change the backup capacity in the Customer solution via the Service Request process.

**Exclusions**

SCC will provide support for all aspects of the solution as defined within scope of the service. The Service Levels Agreements (SLA’s) will measure SCC’s success in the delivery of those services.

Where external factors influence SCC’s ability to deliver against the contractual defined Service then SCC will not be liable for failure to meet the associated SLA’s. These include but are not limited to the following circumstances:

- 3rd Parties, not engaged by SCC, fail to deliver services in accordance with their contractual commitments
- 3rd Parties use of the Sentinel environment outside recommended best practice
- Where the workload or the levels of utilisation of the VM’s cause the system to become unresponsive or suffer from poor performance and where those levels of utilisation are deemed outside of the forecasted demand or sizing criteria of the service
- Where customer requested configuration changes cause application downtime
- Application Configuration causes Operating System instability
- Application Level and End User Testing of all patches and security updates

Any materials and labour provided in these circumstances will be subject to agreement of the parties in writing and;

- Provided on a reasonable endeavours basis (i.e. outside of the Service Levels) unless agreed otherwise by SCC in writing, and
- Charged as additional Ad-hoc Charges.

**7.3 On Boarding**

The scope of this process covers the steps required to establish a new virtual machine within the SCC environment. The process caters for 3 integration scenarios:

- Integration of an existing virtual machine from within the Customers estate
- Integration of an existing physical machine from within the Customers estate
- Creation of a new VM within the SCC environment from an existing Sentinel Template
In all cases an initial discovery phase is required to determine the platform and resources that must be allocated from the environment to the Virtual Machine in order to define the setup activities and charges.

The information established in discovery shall specify:

- CPU Resources
- Memory Resources
- Network Interfaces
- Storage Requirements, including:
  - Data sizes and growth - so capacity can be allocated/planned
  - Performance requirements - space provisioned on correct storage tier
  - Specific requirements due to application nature
  - Security requirements
  - The server(s) that the data/capacity is associated with
- Backup Requirements, including:
  - Required recovery requirements - retention period
  - Nature of data being backed up - security and encryption levels
  - Tape storage needed for off-site storage (will dictate location and security requirements)
  - Requirement for intelligent backup via agents - need for brick level restore, need for quiescing data/applications during backup
  - Other customer specific requirements
- Setup activities and resources
- Connectivity Requirements

This information shall be supplied by the Customer either based on the existing server requirements or via a capacity planning exercise.

Where appropriate, existing servers need to be encapsulated within VMware virtual machine files (VMDK files) or OVF files for incorporation into the platform.

- Existing VMDK or OVF files can be provided by the Customer directly for incorporation into the platform, should this be required (supported operating systems only)
- Other virtual machine formats are to be converted to VMDK or OVF prior to presentation
- Physical servers must be migrated to VMDK or OVF format using an appropriate tool (e.g. VMware Converter) or Deployed as Physical Assets (DPA)

For the latter two options SCC can provide a chargeable service to create the VMDK files or host DPA.

Where data has been encapsulated within the VM file, the security requirements must be assessed to ensure that an appropriate data transfer mechanism (i.e. encryption and security measures) is employed during the transfer of the virtual machine file to our environment. Transfer shall be achieved
through providing the VM file on removable disk media (magnetic or optical) or transmission over a suitable network connection.

When new virtual machines are to be created, SCC shall deploy the server within the environment from a library of hardened and approved server templates.

The resulting virtual machine shall then be validated to ensure that it has been correctly integrated within the environment.

Compliance with Vendor software licensing terms may require SCC to apply additional licensing charges.

### 7.4 Off-boarding

The scope of this process covers the steps taken to remove a virtual machine and associated storage and back up from the SCC environment and return to the customer or deleted if authorised. This would be operated via the Change Management Process.

The virtual machine shall be assessed to determine if there is any data encapsulated within the virtual machine file and, if so, determine the security requirements applicable to the data. This will ensure that appropriate measures (security, encryption etc.) are applied when transferring the virtual machine file back to the Customer.

Where the customer has specified off-site media storage as part of the services or where retention period requirements have dictated media based backup storage then the media will be retrieved and provided to the customer in the format used by our backup software. The data stored on the media shall already have been encrypted to a suitable level and therefore additional encryption measures will not be used when returning media to the customer.

The virtual machine file, together with the associated virtual machine configuration file shall be supplied to the Customer using either removable disk or optical media encrypted as appropriate.

The Customer shall be responsible for validating the integrity of the returned virtual machine file and data – note that this step refers to the confirmation that a valid VM file has been supplied. SCC will not be responsible for ensuring that the virtual machine encapsulated within the file is correctly configured for any environment outside of SCCs service provision.

Where a software license for the operating system or layered software within the VM file has been rented from SCC under a License Agreement the license key shall be removed prior to the return of the VM file.

SCC will then destroy all live and backup copies of the virtual machine file and data within our control in line with CESG guidelines and provide written confirmation to the Customer that this has been performed.

Any On Boarding or Off Boarding process is not part of the Monthly unit rate and will be undertaken as part of a project activity.

### 7.5 Data Restoration / Service Migration

Where data needs to be restored to the operational service from a backup, this shall be requested by the Customer through the SCC Service Desk.
Recovery of data from backup shall be actioned within 4 Hours from the point of request by the customer through the SCC Service Desk for the Basic, Standard and Enhanced Services.

The time required to restore the data will be dependent upon a number of factors including; the amount of data being restored and the complexity of the data restore process.

Service migration shall be possible after completing the data extraction process at which point the data will be available in an appropriate format to migrate to an alternative service, should the customer require assistance with this process SCC can provide migration services at additional cost.

7.6 Termination

A G-Cloud service shall commence on the Effective Date and shall, unless specified otherwise in the Order Form, continue for the Initial Term and shall remain in force thereafter unless and until terminated by either Party giving to the other not less than 30 days written notice, but shall be subject to earlier termination as referenced within the Termination/Consequence of Termination section of the standard SCC G-Cloud terms and conditions.

7.7 Ordering and Invoicing Process

SCC will provide ordering of G-Cloud services via an Account or Customer Service Manager.

A list of G-Cloud services can be compiled with quotations for those specific services. Once The Customer is satisfied that the requirement is met, it can then be converted into an order.

Once the services are enabled and confirmation of the ordered G-Cloud services is delivered to The Customer a monthly invoice in arrears will be generated against the order.

Should The Customers usage of the Service increase or decrease from the contracted volumes during any period then this will be reflected in the next monthly invoice.

7.8 Financial Recompense Model

Service Credits

1.1. Subject to Clause 1.3 below, in the event that SCC fails to meet the SLA Target for the applicable Service Level", then the Service Credit mechanism in Clause 1.2 shall apply

1.2. SCC shall provide a rebate of 1% of the Monthly Charge for this Service, which is applicable over the Report Period for every 1% below the SLA Target to a maximum of 10 % rebate. The applicable Service Credit shall be deducted off the next invoice due to the Customer

1.3. Payment by SCC of Service Credits to the Customer shall be in full and final settlement of SCCs liability to the Customer for failure to meet the Service Levels during the Report Period

1.4. Service Levels will only be calculated against platform availability and not against application availability. Service penalties against the loss of platform availability will not include other machines or applications impacted by that loss

1.5. Service Credits will not be applied where it is determined that SCC are not responsible for the cause of the breach in Availability performance
7.9 Training
There is no training required within this secure service.

7.10 Trial Service
There is no option to consume this service for a trial period.
For more information contact

Kelvin Ayre

gcloud@scc.com

0121 766 7000