SERVICE DEFINITION

G-CLOUD 7

Skyscape Secure Remote Access
CONTENTS

WHY MDS? ........................................................................................................................................... 3

SUMMARY OF SERVICE BENEFITS ........................................................................................................ 3

MDS AND SKYSCAPE – THE PERFECT PARTNERSHIP ........................................................................ 4

WHAT IS THE SERVICE? ............................................................................................................................ 4

WHAT CAN I DO WITH THIS SERVICE? .................................................................................................... 4

WHAT ARE THE KEY FEATURES AND BENEFITS? .............................................................................. 4

WHY SKYSCAPE? ..................................................................................................................................... 5

WHAT ARE THE KEY TECHNICAL FEATURES? ....................................................................................... 6

WHO IS THE SERVICE AIMED AT? ............................................................................................................. 6

WHAT ARE THE SERVICE LEVELS? .......................................................................................................... 6

ROLES AND RESPONSIBILITIES ............................................................................................................ 7

HOW MUCH DOES IT COST? ...................................................................................................................... 8

IS THERE A TRIAL SERVICE? ..................................................................................................................... 10

WHAT ARE THE TERMS AND CONDITIONS? ............................................................................................ 10

APPENDIX .................................................................................................................................................. 11
WHY MDS?

- Bespoke cloud solutions that fit your business needs
- Trusted provider of agile, scalable and assured digital services
- Full range of cloud hosting and enablement solutions
- Security Cleared (SC) operational support staff
- Honest providers of services, support and practical advice
- 24/7 support through our ITIL-aligned Service Desk
- A privately owned, UK sovereign company
- We are an SME - agile with minimal bureaucracy
- Providing infrastructure services to the Public Sector for over 12 years
- Certified against ISO 27001, ISO 9001, ISO14001 and Cyber Essentials Plus
- We listen to our customers, we understand, we deliver

PROFESSIONAL, PERSONALISED SOLUTIONS

SUMMARY OF SERVICE BENEFITS

- A secure remote access solution that uses CESG Assured VPN technologies and the secure ‘walled garden’ architectural pattern
- Flexible connectivity for remote administrators and mobile workers to the Skyscape Elevated OFFICIAL (formerly IL3) cloud platform
- Optimised for OFFICIAL — hosted in the UK and operated by UK government security-cleared staff, the service benefits from extensive independent validation (including CESG Design Review) that it is properly aligned with CESG Cloud Security Principles, making it ideal for remote access to systems classified at OFFICIAL (including OFFICIAL SENSITIVE)
- Provided as a cloud service — no need to purchase and manage CESG-approved VPN hardware
MDS AND SKYSCAPE – THE PERFECT PARTNERSHIP

MDS technologies Limited (MDS) offers a cloud platform provided by the award winning Skyscape Cloud Services (Skyscape). We have a strong, committed relationship with Skyscape, the market leader in the Digital Marketplace for G-Cloud Infrastructure as a Service, through a long-standing relationship underpinned by a formal partnering agreement. We have been a Skyscape Partner since their creation in 2011, and have resold services since the launch of the G-Cloud framework in February 2012. MDS is a reseller, at cost, of Skyscape’s cloud services and is currently Skyscape’s largest partner and second largest consumer of cloud services. This status enables us to provide a high level of service to our customers and gain enhanced support from Skyscape.

As a Skyscape partner, MDS offers true National Institute of Standards and Technology (NIST) cloud services, which are offered as part of a community cloud service only available to the UK Public Sector and secured and managed in line with UK government security classifications.

Skyscape and MDS both utilise pricing models based on transparent charges and “pay for what you use” on an hourly and/or monthly basis.

WHAT IS THE SERVICE?

The Skyscape Secure Remote Access service enables customers to securely connect to the Skyscape Elevated OFFICIAL (formerly IL3) cloud platform using CESG-approved internet virtual private network (VPN) technologies and the ‘walled garden’ architectural pattern (for example, support for bastion hosts).

WHAT CAN I DO WITH THIS SERVICE?

The service enables system administrators and mobile and remote workers to securely access workloads running on the Skyscape Elevated OFFICIAL cloud platform from locations that don’t have alternative secure network connections (such as PSN or N3).

Skyscape’s Secure Remote Access:

- Is available to users who have been appropriately vetted and security cleared as assured by the customer organisation in line with PSN IA conditions
- Can be used by people in the UK and safe harbour countries
- Provides connectivity into the Skyscape Elevated OFFICIAL cloud platform only — there is no onward connectivity to government community networks such as PSN Assured, PSN Protected, legacy networks such as PNN, or N3

WHAT ARE THE KEY FEATURES AND BENEFITS?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexibility</td>
<td>Scale the service as you wish — don’t be restricted by third-party suppliers of access devices</td>
</tr>
<tr>
<td></td>
<td>Manage and assure your devices yourself — no need to mandate the use of inflexible, locked-down devices managed by a provider</td>
</tr>
<tr>
<td>Cross-platform compatibility</td>
<td>Choose the tools that are right for your workforce — Secure Remote Access is compatible with a variety of end-user platforms including Android, Apple, Linux and Microsoft Windows</td>
</tr>
<tr>
<td>Cost-effectiveness</td>
<td>Leverage Skyscape’s ready-made solution to reduce your own infrastructure and compliance costs</td>
</tr>
<tr>
<td></td>
<td>Use a cloud service which provides secure access via a shared multi-tenant CESG-approved internet VPN solution</td>
</tr>
</tbody>
</table>
WHY SKYSCAPE?

Skyscape is a UK company founded in 2011. It is unique among cloud providers as we maintain an exclusive focus on the UK public sector. Skyscape was one of the first G-Cloud providers to successfully achieve CESG Pan Government Accreditation.

Skyscape’s range of on-demand, pay-for-what-you-use, cloud services with no minimum commitment are suitable for OFFICIAL and OFFICIAL SENSITIVE (formerly IL0 through IL4) data. They are delivered from two secure Tier 3 UK data centres separated by more than 100km and securely connected by dedicated high-bandwidth, low-latency CESG-assured circuits, enabling synchronous replication.

Skyscape helps public sector organisations lower CO₂ emissions through reduced energy consumption, sustainable procurement and better hardware utilisation. Skyscape is a CarbonNeutral® Company whose data centres have a low carbon footprint and low PUE rating, and comply with the EU Data Centre Code of Conduct.

Skyscape has unparalleled capability in:

Security assurance
Skyscape offers its cloud services from UK data centres, operated by UK government security-cleared staff. Customers’ data is therefore not subject to foreign legislation or the risk of international surveillance or disclosure.

Services are designed and built with clear alignment to the 14 CESG Cloud Security Principles that all UK public sector organisations use when assessing cloud hosted solutions. The Skyscape cloud benefits from extensive independent validation via certifications ranging from international standards (for example, ISO 9001, ISO 27001, ISO 20000) to UK public-sector specific standards (for example, PSN, N3/HSCIC).

The cloud platforms are subject to regular, extensive IT Security Health Check (ITSHC) CHECK Tests by independent, CESG-approved assessors to provide our customers with confidence in the physical and technical security controls which have been implemented to protect their valuable data assets.

Connectivity
Both UK data centres have resilient connections to secure UK government networks such as PSN Assured, PSN Protected and N3, as well as large-scale, DDoS-protected internet connectivity. This makes it possible for you to present your own connections (such as direct connectivity into your MPLS, or inexpensive point-to-point connections via leased lines); and offer a Secure Remote Access solution that allows assured VPN access to the Elevated OFFICIAL domain.

Flexibility
Skyscape offer simple products for delivering complex solutions, all designed to reduce security risks without decreasing the flexibility of a cloud platform. Differentiated, commoditised products provide a choice of IaaS, PaaS and SaaS; service levels; virtual machine sizes; and security levels.

Innovative solutions further increase cloud flexibility, such as the Cross Domain Security Zone which enables internet-facing Assured OFFICIAL applications to connect to data stored within the Elevated OFFICIAL platform. This allows you to keep your data safe, while letting citizens interface with the information they need.
Public sector partnerships
Skyscape have a committed team focused on identifying partners who understand the UK public sector and have expertise in enabling and accelerating digital transformational projects.

- Managed Service Providers (MSPs). Specialists in services relating to the design, management and support of environments built within Skyscape’s cloud platform, helping to reduce the complexities of platform management.
- Systems Integrators (SIs). Organisations that fully understand Skyscape’s cloud portfolio are experts at bringing together individual cloud components to deliver entire cloud-based solutions.
- Developers and Independent Software Vendors (ISVs). Able to provide fully packaged applications or SaaS solutions which leverage Skyscape’s secure cloud capabilities.
- Strategic Advisors/Consultants. For customers who require additional advice around delivering solutions in the cloud, consultancy partners and subject specialists can help define strategy, develop action plans and create solutions.

WHAT ARE THE KEY TECHNICAL FEATURES?
The Skyscape Secure Remote Access Service:

- Is based on CESG-approved CPA technology including Cisco AnyConnect and Cisco VPN gateways
- Provides secure authentication using two-factor authentication based on Skyscape-issued device certificates
- Has a ‘walled garden’ architecture which enables customers to deploy and manage appropriate systems in a DMZ, allowing secure, controlled onward access to workloads hosted on the Skyscape Elevated OFFICIAL cloud platform
- Is integrated with the Skyscape Protective Monitoring solution (aligned with GPG13)

WHO IS THE SERVICE AIMED AT?
Secure Remote Access provides customers with a simple way to deliver solutions that require a higher level of assurance owing to data sensitivity, with no need to invest in expensive network solutions. Examples of how the service can enable customer success include:

- Organisations whose system administrators and mobile and remote workers need secure connectivity to the Skyscape Elevated OFFICIAL cloud platform
- Organisations looking to enable bring your own device (BYOD) initiatives to avoid being constrained by end-user devices that are too locked down for use by power users (such as developers and system administrators)
- Organisations that want to avoid the cost and complexity of buying, managing and maintaining CESG-approved VPN hardware

WHAT ARE THE SERVICE LEVELS?
Skyscape provides an availability SLA and a response time SLA for the Secure Remote Access Service:
STANDARD

<table>
<thead>
<tr>
<th>Availability (monthly*)</th>
<th>99.90%</th>
</tr>
</thead>
</table>
| Incident response       | P1 — within 15 minutes  
P2 — within 4 hours  
P3 — within 24 hours  
P4 — within 72 hours |
| Service Credits         | 10% of monthly spend on the Secure Remote Access Service |

* Availability indication is based on an average 730 hours per month. Excludes planned and emergency maintenance.

Unavailability applies to the Secure Remote Access VPN end-points due to a fault recognised at the IaaS layer or lower, for example:

- The fault is not caused by the customer (OS, applications, user networks)
- The fault is within Skyscape-controlled components, such as the virtual infrastructure, storage, power or physical firewalls and routers
- External connectivity providers (such as internet) are also not included in the availability calculation

Skyscape also provides an availability service level target on the Skyscape Portal covering the ability to log on to the portal to create support tickets and use other functions.

<table>
<thead>
<tr>
<th>Target availability (monthly*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Portal availability (monthly)</td>
</tr>
</tbody>
</table>

* Availability indication based on an average 730 hours per month. Excludes planned and emergency maintenance.

ROLES AND RESPONSIBILITIES

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provision of end-user device</td>
<td>Customer</td>
</tr>
<tr>
<td>Configuration and management of end-user device</td>
<td>Customer</td>
</tr>
<tr>
<td>Vetting of users of the Secure Remote Access service</td>
<td>Customer</td>
</tr>
<tr>
<td>Assurance/accreditation of users and end-user devices</td>
<td>Customer</td>
</tr>
<tr>
<td>Provision of CESG-approved internet gateway service</td>
<td>Skyscape</td>
</tr>
<tr>
<td>Provision of two-factor authentication solution for device-to-service</td>
<td>Skyscape</td>
</tr>
<tr>
<td>Provision of two-factor authentication solution for user-to-service</td>
<td>Skyscape, customer or MDS</td>
</tr>
<tr>
<td>Provision of ‘walled garden’ environment for customer systems</td>
<td>Skyscape</td>
</tr>
<tr>
<td>Configuration and management of application services in ‘walled garden’</td>
<td>Customer or MDS</td>
</tr>
</tbody>
</table>

The service is compatible with customer-managed end-user devices that meet the following conditions:
- Mandatory use of Cisco AnyConnect VPN Client or an embedded IPsec client which is assured under the CESG CPA scheme against the IPsec VPN for remote working software client security characteristic
- Mandatory user-to-device authentication ensuring only authorised users can access the end-user devices
- Mandatory user-to-service authentication ensuring only authorised users can access the Secure Remote Access Service
- Mandatory device-to-service authentication ensuring only authorised end-user devices can access the Secure Remote Access Service
- Mandatory use of a platform which supports platform integrity and application sandboxing to reduce the risk of the end-user device being compromised
- Mandatory use of application whitelisting to reduce risk of malicious code execution on the end-user device
- Mandatory use of regularly updated anti-malware software to reduce the risk of malicious code execution on the end-user device
- Mandatory use of enterprise-enforced security policies ensuring that end-users cannot override or reconfigure security-critical features
- Mandatory use of external interface protection such as host-based firewalls to limit exposure of the end-user device to untrusted networks
- Mandatory use of a device update policy to keep the end-user device regularly updated with security patches
- Mandatory implementation of an incident response plan by the customer organisation to respond to security incidents such as loss of the end-user device
- Assurance by the consuming organisation that the configuration and management of end-user devices is in line with CESG End User Device guidance and compliant with PSN IA conditions
- Recommended use of a CPA-approved data-at-rest encryption solution
- Recommended use of Secure Boot where available
- Recommended use of an enterprise audit and monitoring service by the customer organisation to ensure security events are centrally logged and reviewed

**HOW MUCH DOES IT COST?**

The Skyscape Secure Remote Access Service is priced as follows:

<table>
<thead>
<tr>
<th>Remote Access pack</th>
<th>Monthly price*</th>
<th>Effective monthly price per certificate*</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 licences</td>
<td>£350</td>
<td>£116.67</td>
</tr>
<tr>
<td>10 licences</td>
<td>£500</td>
<td>£50.00</td>
</tr>
<tr>
<td>25 licences</td>
<td>£1,000</td>
<td>£40.00</td>
</tr>
<tr>
<td>100 licences</td>
<td>£2,500</td>
<td>£25.00</td>
</tr>
<tr>
<td>1,000 licences</td>
<td>£5,000</td>
<td>£5.00</td>
</tr>
</tbody>
</table>

* Prices are per calendar month or part thereof
The prices above include:

- Access to managed CESG-approved VPN gateways
- Cisco AnyConnect licence for the end-user device
- Two-factor authentication using device certificates
- A ‘walled garden’ virtual data centre where customers can deploy their application services

Additional costs for the ‘walled garden’ apply as per the following table:

<table>
<thead>
<tr>
<th>VM Size</th>
<th>vCPU (2GHz)</th>
<th>RAM (GB)</th>
<th>STANDARD (per month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tiny</td>
<td>1</td>
<td>2</td>
<td>£150.00</td>
</tr>
<tr>
<td>Small</td>
<td>2</td>
<td>4</td>
<td>£250.00</td>
</tr>
<tr>
<td>Medium</td>
<td>4</td>
<td>8</td>
<td>£350.00</td>
</tr>
<tr>
<td>Medium High Memory</td>
<td>4</td>
<td>16</td>
<td>£500.00</td>
</tr>
<tr>
<td>Large</td>
<td>8</td>
<td>16</td>
<td>£750.00</td>
</tr>
<tr>
<td>Large High Memory</td>
<td>8</td>
<td>32</td>
<td>£1,000.00</td>
</tr>
<tr>
<td>Tier 1 Apps Small</td>
<td>8</td>
<td>48</td>
<td>£1,500.00</td>
</tr>
<tr>
<td>Tier 1 Apps Medium</td>
<td>8</td>
<td>64</td>
<td>£2,000.00</td>
</tr>
<tr>
<td>Tier 1 Apps Large</td>
<td>8</td>
<td>96</td>
<td>£3,000.00</td>
</tr>
</tbody>
</table>

**Worked example**
The customer requires a Secure Remote Access Service for 105 named users and devices. The customer will run two x Medium sized VMs in the ‘walled garden’ as Bastion hosts.

The customer buys:

- 1 x 100 licences @ £2,500 per month
- 1 x 10 licences @ £500 per month
- 2 x Medium VMs @ £350 each per month = £700 per month
- Total = £3,700 per month

**Cloud Credits**
The Cloud Credits option allows organisations to purchase Cloud Credits upfront and redeem them against Skyscape cloud services over a maximum two-year period. This allows organisations to effectively commit their CAPEX or budget spend in advance, with monthly usage deducted from the balance until depleted.

- Every £1 spent on Cloud Credits equals £1 to be spent on Skyscape cloud services
- The purchase of Cloud Credits can be made against any G7 Service Description, and Cloud Credits are transferable between services
- Cloud Credits can be used for a single service or a combination of services or orders
- Any unused Cloud Credits at the end of the two-year period are non-refundable
**Worked example**
If you know you will consume at least £550,000 of Skyscape cloud services over a two-year period based on previous or projected usage, you may choose to pre-pay this amount. You will receive a value of £550,000 worth of Cloud Credits to be used against any Skyscape service over a maximum two-year period.

You will receive a monthly invoice, with payment automatically taken from your Skyscape Cloud Credits, if available. You will need to inform our finance department if you wish to make any amendments to how your invoices are paid.

**Ancillary options**
The Skyscape Pricing Guide is a comprehensive catalogue of pricing. It includes all ancillary service options available for use with the Skyscape Secure Remote Access service.

Ancillary options include:
- Connectivity options, such as HybridConnect, PSN, N3, internet, data centre interconnect
- SFIA rate card for ad-hoc services

Other ancillary options are available — see the Skyscape Pricing Guide.

**IS THERE A TRIAL SERVICE?**
Skyscape offers a 30-day free trial

Free Trial conditions, as outlined in Appendix A of Skyscape's Standard Terms and Conditions, apply.

**WHAT ARE THE TERMS AND CONDITIONS?**
Please refer to the terms and conditions document for full details.

The appendix at the end of this service description provides a service summary.
APPENDIX

On-boarding and off-boarding

On-boarding
Given the nature of this service, on acceptance of an order, Skyscape will work with the customer to create an assurance plan for the Secure Remote Access service to include the customer’s end-users and associated devices. The assurance plan will include:

- Validation of requirements by the HMG customer (for example, department SIRO)
- Evidence from the customer that end-user devices are configured and managed in line with minimum requirements (for example, scope of PSN compliance with IA requirements)
- Evidence from the customer that users of the Secure Remote Access service are vetted and security cleared in line with minimum requirements (for example, scope of PSN compliance with IA requirements)
- Confirmation by the customer that an appropriate security incident management process applies to this solution
- Confirmation by the customer that the service will be accessed from the UK and safe harbour countries only
- Confirmation by the customer and each individual user of agreement to Skyscape Acceptable Use Policy (AUP)
- Identification of data flows between the ‘walled garden’ and the customer’s solution (for example, firewall access control list)

Skyscape will create the customer’s Primary Administrator account and send a Welcome Pack which includes the URL for the Skyscape Portal for access to the knowledge centre and service management function.

The customer’s Primary Administrator can then provide details of each named user and associated end-user device to be enrolled onto the Secure Remote Access Service.

Off-boarding
On termination of the Secure Remote Access service, Skyscape will:

- Revoke all user and device certificates associated with the solution
- Disable all user accounts
- Remove access control lists from ‘walled garden’ firewalls
- Deleted the ‘walled garden’ virtual data centre

Service constraints
The Skyscape Secure Remote Access service can be used only for connectivity to Skyscape services such as Compute-as-a-Service, Hadoop in the Cloud.

The service is designed to operate only when the following constrains are met:

- Configuration and management of end-user devices is assured by the customer organisation to be in line with CESG End User Device guidance, compliant with PSN IA conditions, and compliant with the ‘Technical requirements’ section below
- The service is available for use only by users who have been appropriately vetted and security cleared as assured by the customer organisation in line with PSN IA conditions

Skyscape will adhere to the following in terms of maintenance windows:

“Planned Maintenance” means any pre-planned maintenance of any infrastructure relating to the services. Skyscape shall provide the customer with at least twenty four (24) hours’ advance notice of any such Planned Maintenance.
Planned Maintenance of Skyscape’s infrastructure relating to the services shall happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on a Saturday and/or Sunday. No Planned Maintenance will take place on a Saturday unless agreed in advance by both parties.

Planned Maintenance shall be excluded from any availability calculation in regard to Service Credits but shall be included in the monthly service reporting.

“Emergency Maintenance” means any emergency maintenance of any of the infrastructure relating to the services. Whenever possible, Skyscape shall provide the customer with at least six (6) hours’ advance notice.

Whenever possible Emergency Maintenance of Skyscape’s infrastructure will happen between the hours of 00:00 and 06:00 (UK local time) Monday to Sunday and/or between the hours of 08:00 and 12:00 (UK local time) on Saturday and/or Sunday, unless there is an identified and demonstrable immediate risk to a customer’s environment.

Emergency Maintenance shall be excluded from any availability calculation in regard to Service Credits but shall be included in the monthly service reporting.

**Training**

Skyscape has created a number of videos, help guides, manuals and FAQs to help train and instruct users so that they are up and running quickly and easily.

Skyscape also has a number of Partners who can deliver additional services such as training, support and managed services. Skyscape would be pleased to introduce you to such Partners where appropriate.

**Ordering and invoicing**

Billing for the service is:

- Monthly in arrears for monthly fees

Payment can be made by direct bank transfer (BACS/CHAPS).

**Service lead time**

Setting up a new customer on the Skyscape Portal will typically be completed within 4 hours of order acceptance.

Resources to validate the assurance plan activity will be assigned within 10 days of order acceptance.

Given the variable nature of this service, full on-boarding of the customer organisation including enrolment of users and end-user devices will take an indeterminate amount of time.

**Termination**

**Terms**

The service is subject to a minimum term of three months. Termination within this initial term will incur an early exit charge.

Customers are required to provide notice of termination of not less than 10 working days.

At the point of termination, customers must ensure that they have extracted any required data from the ‘walled garden’ virtual data centre as Skyscape will ensure all customer data, accounts and access will be permanently deleted, and will not be able to subsequently recover or restore them.

**Costs**

An early exit charge will be payable if the contract is terminated within the minimum term. The early exit charge will be equal to the cost of three months’ service less payments already made.

Customers are responsible for extracting their own data from the platform if required.

Skyscape may make an additional charge for transferring data out of the service.

**Customer responsibilities**

- The control and management of access and responsibility for end-users including appropriate connectivity, security and assurance/accreditation if
required. If access is required over Government Secure Networks such as N3, PSN, the customer is responsible for adhering to the Code of Connection.

- Providing details of all devices to be enrolled onto the service. Management and administration of end-user devices including ensuring that security policies remain in effect, security patches are regularly applied and anti-malware software is up-to-date. Refer to the ‘Service constraints’ section for additional information.

- Providing details of all users to be enrolled into the service. Ensuring all users of the service are vetted and security cleared as appropriate. Ensuring all users receive regular information security training.

- Ensuring the service is used from within the UK and safe harbour countries only.

- Providing a suitable internet connection to enable end-user devices to connect to the Skyscape Secure Remote Access service.

- Providing access requirements between the ‘walled garden’ and customer solutions (for example, firewall ports).

- Management of security incidents related to the use of this service (for example, lost end-user devices)

- The customer is also responsible for ensuring only appropriate data (OFFICIAL or OFFICIAL SENSITIVE) is stored and processed by applications on this environment and that they comply with the Skyscape Security Operating Procedures (SyOps) and other information assurance requirements as specified in Skyscape System Interconnect and Security Policy (SISP) and associated accreditation documentation sets.

**Data restoration / service migration**

For service migration, Skyscape allows existing data to be migrated to and from the ‘walled garden’ virtual data centre.

In many circumstances, Skyscape can help facilitate a bulk migration to the platform using offline data ingest and extraction — please ask Skyscape for details.

**Financial recompense model**

If the service level falls below the stated availability percentage (excluding Planned and Emergency Maintenance periods), customers will be eligible for Service Credits on affected storage only. Service Credits will be calculated as a percentage of the fees for the affected services for the monthly billing period during which the failure occurred (to be applied at the end of the billing cycle).

<table>
<thead>
<tr>
<th>Service Credit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Remote Access service</td>
<td>10% of monthly spend on this service</td>
</tr>
<tr>
<td>Customer Portal</td>
<td>1% of monthly spend per 1% below service level target or part thereof</td>
</tr>
</tbody>
</table>

**Technical requirements**

Customers must provide end-user devices which meet the requirements of this service:

- Mandatory use of Cisco AnyConnect VPN Client or an embedded IPsec client which is assured under the CESG CPA scheme against the IPsec VPN for Remote Working Software Client security characteristic.

- Mandatory user-to-device authentication ensuring only authorised users can access the end-user devices

- Mandatory user-to-service authentication ensuring only authorised users can access the Secure Remote Access Service

- Mandatory device-to-service authentication ensuring only authorised end-user devices can access the Secure Remote Access Service

- Mandatory use of a platform which supports platform integrity and application sandboxing to reduce the risk of the end-user device becoming compromised
• Mandatory use of application whitelisting to reduce risk of malicious code execution on the end-user device

• Mandatory use of regularly updated anti-malware software to reduce risk of malicious code execution on the end-user device

• Mandatory use of enterprise-enforced security policies ensuring that end-users cannot override or reconfigure security-critical features

• Mandatory use of external interface protection such as host-based firewalls to limit the exposure of the end-user device to untrusted networks

• Mandatory use of a device update policy to keep the end-device regularly updated with security patches

• Mandatory implementation of an incident response plan by the customer organisation to respond to security incidents such as loss of the end-user device

• Recommended use of a CPA-approved data-at-rest encryption solution

• Recommended use of Secure Boot where available

• Recommended use of an enterprise audit and monitoring service by the customer organisation to ensure security events are centrally logged and reviewed