Managed AWS for UK Public Sector Service Terms

These service terms cover only Sungard Availability Services' (Sungard AS') Managed AWS for UK Public Sector and, depending on network services, must be taken together with the Public Sector Network ("**PSN**") Networking Services described in section 3 of this document.

Unless otherwise specified, any of the Services specified in Sections 2, 3, 4, 5 and 6 are provided only if specifically selected in the Order.

Managed Cloud — AWS Terms, and AWS Reseller License Terms take precedence over these terms for contracted service elements consumed on the Amazon Web Services (AWS) platform.

The Term and each renewal period, as set out in the Order for these Services, may not exceed the maximum duration allowable under the UK Government G-Cloud Framework.

On expiration or termination of the Order for any reason and provided Customer is not in default of its payment obligations under the Order or any other Order with Sungard AS, Sungard AS will provide Customer with reasonable and orderly transition services ("**Transition Services**") as well as information and documentation as agreed and defined on the Commencement Date the Customer requires in connection with the orderly and expeditious transition of Services. Excluding information that is commercially sensitive or of a proprietary nature to Sungard AS, the Transition Services will be provided for a period of up to one hundred and twenty (120) days, provided Customer continues to make timely payments of the fees attributable to the Services on a pro-rata basis.

Notwithstanding anything to the contrary, if Customer terminates the Order prior to the end of the Term for any reason, Customer acknowledges that it is responsible for payment to Sungard AS of all charges relating to any Customer virtual private cloud (VPC) until it is decommissioned and the associated Sungard AS Equipment, Sungard AS Software and Storage Infrastructure is no longer used by Customer.

1. DEFINITIONS

"**Contended Virtual Machine**" is a virtual machine that has undedicated resources and, therefore, available capacity at peak times may influence performance.

"**Core OS**" refers to the core components of the basic installation of an OS, excluding additional server "roles" such as DHCP server, DNS server and Internet Information Server.

"**Customer Designees**" refers to any of the Customer's employees, consultants, contractors, agents and other authorized representatives as the Customer may periodically notify Sungard AS in writing of these individuals needing access to the Customer virtual data center(s) (VDC(s).

"**Customer Portal**" is a web-based service portal accessible via the PSN Network that Sungard AS provides to the Customer to access information in relation to Managed AWS for UK Public Sector.

"**Customer Software**" refers to Customer-provided software.

"**Equipment**" refers to the Sungard AS Equipment.

"**IaaS**" is Infrastructure as a Service.

"**Managed AWS for UK Public Sector**" refers to the "Services" as set out herein and incorporating IaaS and PaaS.

"**Managed Physical Host**" is a physical machine that provides a system which supports the execution of a complete OS dedicated to one customer.

"**PaaS**" is Platform as a Service, where Sungard AS manages the OS and/or application/software (not the Customer end-user application/software) in the Customer's VDC on their behalf.

"**Policies**" refers to all reasonable rules or instructions given by Sungard AS, including Sungard AS' site access, security, confidentiality, operational, health and safety and other regulations in effect, as amended, from time to time.

"**Resilient**" refers to Equipment, Software or infrastructure that is duplicated in such a way as to avoid any single points of failure.

"**Service-Level Commitment**" refers to the target for the provision of particular elements of specific Services.

"**Software**" refers to the Customer Software and Sungard AS Software.

"**Standard Bandwidth**" is the speed (in bits per second) of a communications link as specified in the Schedule.

"**Storage Infrastructure**" is the Sungard AS Storage equipment used to provide the Managed AWS for UK Public Sector to the Customer.

"**Sungard AS Equipment**" is the Sungard AS equipment used to provide the Managed AWS for UK Public Sector.

"**Sungard AS Software**" is the Sungard AS software used to provide the Managed AWS for UK Public Sector.

"**VDC**" is the Customer virtual data center. It will be dedicated to a single customer and hosted on Sungard AS' Managed AWS for UK Public Sector.

"**Virtual Machine**" is a software implementation of a machine (i.e., a computer) like a physical machine that provides a complete system platform which supports the execution of a complete OS).

"**Virtual Firewall**" is the segmentation through virtualization of a physical firewall system to provide a virtual firewall dedicated to Customer.

2. MANAGED AWS FOR UK PUBLIC SECTOR

2.1. Features

The purpose of the Services is to make available to Customer various elements of the following services, if selected in the Order and as supplemented in the sections below:

(a) Network Connectivity Services to allow Customer to connect into the Managed AWS for UK Public Sector platform.
(b) IP Network Services to enable the connectivity and balancing of IP services.
(c) Infrastructure resources and managed services to provide processing and storage functionality for customer systems and the management of these systems.
(d) Storage Services to facilitate the read, write and storage of Customer data.
(e) Incident Resolution Services (as defined herein) to detect and resolve incidents associated with the Services.
(f) Service-Level Commitments to provide high availability of the Network Connectivity and IP Network Services and AWS Infrastructure resources.

2.1.1. Monitoring

The monitoring components of the Managed AWS for UK Public Sector Services may require a monitoring agent be installed on the asset, OS and/or application(s). Customer will install the agent and vendor-required upgrades or updates, unless the asset, OS and/or application(s) are managed by Sungard AS.

Monitoring is conducted at 5-minute intervals. Customer notification is triggered by two consecutive negative polling responses.

Monitoring detects only positive or negative Internet Control Message Protocol / Simple Network Management Protocol (ICMP/SNMP) responses from direct Network Interface Card (NIC)polling. Additionally, devices send SNMP traps that are processed in the same way as polled events. Monitored devices may generate false-positive alerts that are caused by network congestion or application activity.

2.1.2. Support

Sungard AS will provide technical support, problem resolution and change management for the Managed AWS for UK Public Sector Services via our ISO20000-aligned service management solution.

The Services do not include support for configurations or architectures that are not supported or recommended by the applicable vendor.

2.1.3. Infrastructure and Maintenance

From time to time, Sungard AS may need to perform maintenance on or make adjustments to the infrastructure (including, without limitation, any Sungard-AS-provided telecommunications links, Sungard AS Equipment and Sungard AS Software on which the Customer virtual private cloud(s) (VPC(s)) relies) and shall be entitled to do so at its discretion, without incurring liability for so doing. In the event of any such maintenance or adjustment being needed, then, except in the case of emergency maintenance, Sungard AS will give Customer reasonable prior notice and shall use all reasonable endeavors to limit the interruption. If emergency maintenance is needed, Sungard AS shall be entitled to interrupt the Services without prior notice.

2.2. General

2.2.1. Software

For all Sungard AS Software licensed from Microsoft, Customer shall comply with Microsoft's Service Provider Use Rights ("SPUR"), the terms of which are available at http://www.microsoftvolumelicensing.com/, or such other source as Microsoft periodically may make available. Customer will not:

(a) Remove, modify or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Sungard AS Software.
(b) Reverse-engineer, decompile or disassemble the Sungard AS Software, except to the extent that such activity is expressly permitted by applicable law.
(c) Perform any act that is not in compliance with the terms of SPUR.
(d) Use the Sungard AS Software, except as part of the Services.

Customer acknowledges and agrees that, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers is disclaimed for any damages, whether direct, indirect or consequential, arising from Customer's use of the Sungard AS Software. Customer acknowledges that the Sungard AS Software is not fault-tolerant. The Sungard AS Software is neither designed nor intended for use in a situation where its failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High-Risk Use"). Customer is not permitted to use the Services in, or in conjunction with, High-Risk Use. High-Risk Use includes, e.g., aircraft or other modes of human mass transportation, nuclear or chemical facilities and Class III medical devices under the U.S. Food, Drug, and Cosmetic Act. Customer shall indemnify Sungard AS against any loss, damage, cost or expense (including legal costs) that Sungard AS incurs, suffers or becomes liable for as a result of any breach by Customer of Section 2.2.1, which causes a breach of any third party's intellectual property rights.

For all other Sungard AS Software licensed from other providers Customer shall comply with the terms of the license management scheme as detailed herein.

Sungard AS uses software licensed from third parties in providing the Services. Title to the Sungard AS Software remains with Sungard AS or its third-party licensors and is subject to copyright. Customer shall accept and comply with the provisions relating to the Sungard AS Software specified in the Order or otherwise made known by Sungard AS to the Customer in writing. Customer consents to Sungard AS providing details of Customer's name and address to such third parties for reporting purposes.

Where the Services involve the provision of Sungard AS Software, Customer confirms that:

(a) It will not contact the software provider directly, otherwise Sungard AS shall be entitled to charge Customer the cost that Sungard AS incurs from the provider.
(b) That access to the Sungard AS Software will cease upon termination and Customer will not use the Sungard AS Software beyond this period.
(c) It will ensure that it uses the Sungard AS Software in accordance with all applicable laws and regulations.
(d) It will not copy or reproduce in whole or in part, adapt and modify any documentation received regarding the Sungard AS Software.
(e) It will not reverse-engineer, disassemble or decompile the Sungard AS Software, nor attempt to derive or determine the source code or the logic therein.
(f) It will not use the Sungard AS Software other than for its own internal business purposes.
(g) it will not use the Sungard AS Software in association with safety-critical applications that include, but are not limited to, medical systems, transport management systems, vehicle and power generation applications and nuclear power applications.
(h) It will not, in relation to the Sungard AS Software sub-license, rent, sell, lease, distribute or otherwise transfer to a third party.

Database licenses are provided by Customer unless listed in the Order.

2.2.2. Customer Designees

Customer is responsible for ensuring that the list of Customer Designees is up to date at all times, including (without limitation) promptly notifying Sungard AS in writing of any persons who are to be removed from the list. Customer shall not and shall ensure that the Customer Designees shall use the VPC strictly in accordance with the terms of this Agreement (which includes the terms set out in the Customer agreement(s) with AWS for the AWS Infrastructure). If any Customer Designee does something or fails to do something which results in Customer breaching Section 2.2.2 or any other provision of this Order or the Agreement, Sungard AS shall be entitled (without prejudice to any other rights or remedies it may have) to require that such person immediately lose access to the VPC(s). Customer shall not allow any persons, who are not authorized to do so, to gain access. If unauthorized persons gain access to Customer VPC(s), Customer shall be responsible for any resulting loss, damage or expense suffered or incurred by Sungard AS, AWS or any other customers to the Services or any connected services provided by Sungard AS.

2.2.3. Customer Software

Customer shall be responsible for the operation and maintenance of the Customer Software. Customer shall ensure it is lawfully entitled to use the Customer Software on all the Sungard-AS-provisioned resources (including AWS Infrastructure) and that, where necessary, Sungard AS is permitted to use the Customer Software on the Sungard-AS-provisioned resources for the purpose of providing Services to Customer. Customer shall, at Sungard AS' request, promptly provide written confirmation to Sungard AS from the proprietor(s) of the Customer Software of such entitlement and permission. Customer shall indemnify Sungard AS for any loss, damage, costs, claims or proceedings that Sungard AS may incur as a result of any breach by Customer of Section 2.2.3. Customer shall ensure that the Customer Software is compatible with the Services.

Where Sungard AS provides the Managed OS Service, Sungard AS does not include the support of Customer Software installed on the OS. Sungard AS does not guarantee a time to fix Customer Software.

On the expiration/cancellation of an Order for any reason, Customer will delete or migrate all Customer data resident on the Services. Sungard AS will securely delete all Customer data and Customer Software from Customer VPC(s). Sungard AS will not be able to recover any data after this action has been undertaken.

On expiration or termination of the Order for any reason, Customer must immediately discontinue all use of the Services. Sungard AS will remove access to the Customer VPC and de-install all Software.

Sungard AS shall be entitled to audit Customer's use of the Services for the purpose of ensuring the Customer's compliance with its obligations under this Order.

2.2.4. PSN Code of Connection (CoCo) and Compliance

Customer is responsible for maintaining their PSN CoCo to use the Services and must notify Sungard AS if it ceases. Customer must ensure that the OS and application/software that are deployed and supplied by, and on the Sungard AS' Managed AWS for UK Public Sector platform are included in their Information Technology Health Check (ITHC). Customer's ITHC, which covers the platform and applications, will sit alongside Sungard AS; ITHC, which covers the infrastructure (as part of its PSN CoCo), to provide PSN full assurance of the overall Customer solution.

3. NETWORK CONNECTIVITY SERVICES: MANAGED AWS FOR UK PUBLIC SECTOR

3.1. Features

The Network Connectivity Services for Managed AWS for UK Public Sector may include one or more of the services described in the following sub-sections.

3.1.1. PSN Access Services

PSN Access Services include:

(a) Allocated PSN Assured (no encryption) or PSN Protected (with encryption) bandwidth on the applicable AWS region. PSN connections will be provisioned with the specified amount of Bandwidth.
(b) Monitoring of PSN availability to Customer VPC(s).
(c) Usage tracking and reporting of the Standard Bandwidth.
(d) If Réseaux IP Européens (RIPE) IP Addresses are specified, providing the specified number of such addresses.
(e) If PSN Registered Domain Name System (DNS) zones are specified, providing configuration of DNS zones and records in accordance with configuration instructions supplied by Customer for the domains specified and associated with the PSN Access Services.

3.1.2. Inter-site Services

Inter-site Services include:

(a) Provision of routing and firewall management to support Customer application replication traffic.
(b) Usage tracking and reporting of the Standard Bandwidth.

3.1.3. Private PSN Connectivity

If private PSN connectivity is selected in the Order, Customer will procure (or procure through Sungard AS) a private virtual routing and forwarding (VRF) on the PSN as described below to allow for a privately accessible connection to the Managed AWS for UK Public Sector platform. The private VRF will transmit through the PSN Direct Network Service Provider (DNSP) infrastructure and terminate at Customer's wide-area network (WAN) to the VPC(s). The private VRF will terminate onto the AWS Infrastructure and be routed to the Customer VPC

within the Managed AWS for UK Public Sector AWS London region (or another region selected by Customer). Customer will be provided with Virtual Firewall services.

3.1.4. Monitored Links and Managed Services

This section describes when and why Sungard AS monitors links or provides Managed Services (as defined below) for such links. Unless the link complies with the criteria below, Sungard AS will not be able to monitor the link or provide a Managed Service in respect of it.

Sungard AS' ability to monitor a link does not imply that redundancy exists in the service, i.e., a duplication of elements to provide alternative functional channels in case of failure. The link may still be a potential single point of failure.

For certain managed Sungard AS services ("Managed Services"), Sungard AS can take responsibility for the monitoring, performance and maintenance of the Services up to the relevant Sungard AS Demarcation Point, except that its responsibility for the availability, timing or quality of transmission or signalling on the circuit or network may cease at a different point, e.g., the Carrier Demarcation Point at the Customer (or third party) end of the link

3.1.5. Public Service Network (PSN) Traffic Management

Where specified in the Order, Sungard AS will resolve traffic management problems by the application of readily available fixes and patches supplied and supported by the relevant vendors.

3.1.6. Internet Access Services

Sungard AS' Internet Access Services for Managed AWS for UK Public Sector include:

(a) A connection via AWS' public network from the selected AWS region to the Internet.
(b) Monitoring of Internet availability.
(c) Usage tracking and reporting of the Bandwidth.
(d) If Internet IP Addresses are specified in the Order, providing the specified number of such addresses.
(e) If DNS Administration Services are specified in the Order, providing configuration of DNS zones and records in accordance with configuration instructions supplied by Customer for the domains specified in the Order associated with the Dedicated Internet Access Services.

3.1.7. DDoS Mitigation Service

Distributed denial of service (DDoS) mitigation is provided by AWS by default, at no additional charge. AWS standard DDoS mitigation defends against most common, frequently occurring network and transport layer DDoS attacks that target customer web sites or applications.

3.2. General

3.2.1. PSN Access Services General Terms

The Standard Bandwidth provided for PSN Access Services will be capped. Sungard AS shall have no obligation to provide a PSN connection exceeding the Standard Bandwidth unless Customer contracts for additional capacity by way of a written amendment to this Order.

None of the PSN Access Services is owned, operated or managed by, or in any way affiliated with, Sungard AS or any of Sungard AS' Affiliates. The PSN is a dedicated computer network of interoperable packet-switched data networks for use by the UK Public Sector. Sungard AS cannot guarantee that the PSN Access Services from third-party providers are sufficient to meet Customer's needs. Customer agrees that it uses the PSN from third-party providers solely at its own risk and subject to the PSN CoCo and warrants that it will comply with all such requirements as defined by the PSN/Cabinet office in its use of the Services.

Customers consuming the Services in the applicable AWS Region(s) across the PSN are responsible for gaining and maintaining their own PSN connection compliance certification for the end user systems that they deploy on Sungard AS' Managed AWS for UK Public Sector platforms and consume over the PSN.

Sungard AS is responsible for gaining and maintaining its own PSN connection and PSN service-provision-compliance certifications.

3.2.2. Inter-site Services General Terms

Certain Network Services are provided subject to the availability of the necessary services from Sungard AS' telecommunications providers and AWS. Accordingly, Sungard AS does not guarantee (nor is it a condition or warranty of this Order) that transmission of data via the communications links always will be possible without interruption or error. Sungard AS may, by written notice to Customer, terminate or withhold the provision of such Network Services (or any part of them) without liability if:

(a) Sungard AS' telecommunications providers or AWS terminate services to Sungard AS, or withdraw or substantially alter any underlying tariff(s).
(b) Any regulatory authority asserts jurisdiction over the Network Services, with the result that Sungard AS is required to submit to common carrier, public utility or other regulations to which Sungard AS is not then subject.
(c) Sungard AS no longer has the legal right to provide the Network Services.

If requested by Customer, Sungard AS will work with Customer to help it secure replacement Network Services from a replacement telecommunications provider.

Sungard AS' charges are based in part on its telecommunications providers' tariffs and/or charges prevailing at the time the Order was entered into. If Sungard AS' telecommunications providers increase any such tariff(s) or charges beyond those prevailing at the time the Order was entered into, Sungard AS shall be entitled to increase the Charges payable by such amount as will compensate Sungard AS (on a passthrough basis with no profit element) for any such increase and shall not be liable for any consequent delay in the provision of the Services.

3.2.3. RIPE IPV4 (IP Addresses) General Terms

Any RIPE addresses provided by Sungard AS will be from a Sungard AS IP network block and are non-portable. These addresses will be for the use of Customer only and shall not, without Sungard AS' prior written consent (given in Sungard AS' absolute discretion), be used by or assigned to any third party. RIPE addresses allocated by Sungard AS must be returned promptly to Sungard AS if Customer discontinues the applicable Services for any reason or on expiration or termination of the Order.

Sungard AS procures its IPv4 IP address allocation from RIPE. The address allocation is given based on Sungard AS agreement to conform with the policies and guidelines for assignments by RIPE. The number of IPv4 address allocations given by RIPE to Sungard AS is based on the perceived customer usage rates. If Customer does not employ these usage rates, Sungard AS reserves the right to withdraw the unused IP addresses for it to conform with RIPE.

3.3. Network Connectivity Services: Managed AWS for UK Public Sector Service-Level Commitments

3.3.1. Availability of Third-Party Telecommunications Circuits

Target: The target for PSN Network Services procured through Sungard AS is that Services will be operational and available to Customer 98.4% of the time during each calendar month. Where such Network Services are Resilient, the target shall be 99.95%.

Measurement: Availability will be measured from the time the unavailability is reported to Sungard AS by Customer using Sungard AS' reporting procedures. When Sungard AS hands back the circuit for Customer

testing and verification, the circuit is deemed available until the Customer reports otherwise, in which case availability will be re-measured from the time of such report. The percentage availability is calculated as follows:

The denominator of the calculation is the total number of hours in a calendar month, minus:

(a) The total amount of hours used during any preventive maintenance scheduled by Sungard AS or any Customer-requested downtime.
(b) Any time attributable to the Service-Level Exclusions referenced in the Appendix to the Agreement.

The numerator is the total number of hours in a month, minus:

(c) The total amount of hours used during any preventive maintenance scheduled by Sungard AS or any Customer-requested downtime,
(d) Any time attributable to the Service-Level Exclusions referenced in the Appendix to the Agreement.
(e) Any other downtime.

The resulting fraction (multiplied by 100) is the percentage of actual Availability. The connection may, at times, be working despite the measurement showing it to be unavailable. In this case, it will be deemed available if the devices are responsive to work requests.

Remedy*:* If, during any one 1-month period, Availability falls below the applicable target percentage as an average for the month then, for each full hour of unavailability, Sungard AS will credit Customer one day's Charges then payable by Customer specifically for the failed link or, if no such Charges are specified, the applicable percentage of the then-current monthly charges that Sungard AS would charge its customers generally for such link. Customer may claim a maximum of 10 such credits in any one month.

3.4. Managed Firewall Services

The following are included in the Managed Firewall Services:

(a) All equipment and software required to provide the Managed Firewall Services.
(b) Monitoring of the firewall availability.
(c) Firewall rules\policy configuration upon Customer request.
(d) Resolution of firewall incidents.

Customer system administration access to firewalls' infrastructure is not permitted.

3.5. Managed Load Balancing Services

The following are included in the Managed Load Balancing Services:

(a) All equipment and software required to provide the Services.
(b) Monitoring of the load balancing availability.
(c) Load balancer policy configuration upon Customer request.
(d) Resolution of load balancer incidents.

Customer system administration access to the load balancer infrastructure is not permitted

4. INFRASTRUCTURE RESOURCES AND MANAGED SERVICES: MANAGED AWS FOR UK PUBLIC SECTOR

4.1. Compute Resources

Sungard AS is responsible and will maintain the ongoing patches of all OSs and/or application/software templates and the VMs deployed from these templates within the core management zones of the platform.

Sungard AS will undertake an Annual IT Health Check (CHECK) to ensure that the supported OSs and/or the application/software templates and the VMs in the core management zones deployed from these templates are adequately patched to the required state.

4.2. Managed OS Services

Sungard AS will provide the initial OS build and agent installation (if applicable) for the number of VMs identified in the Order.

Sungard AS will provide the following for the number of VMs identified in the Order:

(a) Core OS configuration changes upon Customer request.
(b) Management of Sungard AS system administration access (e.g., root- or administrator-level access) to undertake management of the OS of the VM(s) within Customer VPC(s).
(c) Installation of antivirus software on Microsoft Windows OS servers (for more information, see the Managed Microsoft Runtime Application Services section below).
(d) Monitoring OS patch alerts and providing Customer notification of such patches.
(e) Execution of VM(s) snapshot schedules and retention of the number of snapshots, both as defined by Customer, file restore from snapshots upon Customer request and modification(s) to the snapshot schedule upon Customer request as well as one initial data restoration test.
(f) OS problem resolution and incident management, and monitoring of availability and thresholds identified in the completed customer design requirements (CDR) form as well as Customer notification if Sungard AS detects non-responsiveness or exceeded thresholds.
(g) If Customer purchases Platform as a Service (PaaS), Sungard AS will maintain the ongoing patches of all supported OSs running on the VPC(s) on Customer's behalf, but Customer is responsible for maintaining the ongoing patches of its user applications/systems that sit on top of the platform OSs.
(h) Where the Customer requests Sungard AS not to patch the supported OSs, Sungard AS will inform the PSN if patching is delayed. If the delay exceeds the requirements of PSN, as per the guidelines, Sungard AS reserves the right to suspend the service to Customer.
(i) Customer is also responsible for any CHECK required on its end-user applications, including a CHECK on the OS(s) that is deployed and supplied by, and on the Sungard AS Managed AWS for UK Public Sector PaaS platform. The Customer shall share its CHECK results with Sungard AS on request.

For all VMs receiving Managed Services, Customer will:

(a) Provide verification of the licenses and necessary license keys that are applicable to Customer Software prior to Service provision by Sungard AS.
(b) Provide Sungard AS with system administration access (e.g., administrator- or root-level access) for each VM within the VPC(s) and permit such access to be traced and recorded by Sungard AS.
(c) Obtain and maintain 24x7 maintenance agreements with the original software vendor for Customer Software and notify the vendor of Sungard AS' authorization to act as Customer's agent under the maintenance agreements.
(d) Be responsible for the approval and/or testing of all software patching that is identified as available for installation as part of the Services prior to Sungard AS installing on the live managed OS server. Sungard AS reserves the right to apply critical patches to the managed OS where this is required for security or performance reasons without the Customer having completed its tests.

4.3. Managed Antivirus Services (AVS)

Sungard AS will provide Managed Antivirus Services (AVS) for the number of managed OS instances that Sungard AS manages as specified in the Order.

Managed Antivirus Services include:

(a) Installation and configuration of antivirus software on Sungard-AS-managed OS instances in accordance with Sungard AS' standard minimum configuration.
(b) Identification by the software of software patches and notification of Software updates.
(c) Ongoing signature updates.
(d) Review of alerts and notification of such to Customer to allow incident response and management.

Customer shall authorize the removal or deletion of any identified or infected files on the Customer VM(s) prior to Sungard AS addressing the incident. Infected files will be quarantined pending Customer instructions.

4.4. Managed Microsoft Runtime Application Services

Sungard AS will provide the initial design, build, service set up and ongoing monitoring and management of the supported Microsoft Applications as defined in the Service schedule for the number of VMs identified in the Order.

If Customer purchases the PaaS, Sungard AS will maintain the ongoing patches of all supported application/software running in Customer systems within Customer' VPCs, but Customer is responsible for maintaining the ongoing patches of its user applications/systems that sit on top of the platform OS and/or supported application/software.

If Customer requests that Sungard AS not to patch the supported application/software that is deployed and supplied by Sungard AS, Sungard AS will inform the PSN if patching is delayed where the delay exceeds the requirements of PSN as per the guidelines and reserves the right to suspend the service to the customer.

Customer is responsible for any annual IT Health Check by a CHECK Registered Supplier required on its end-user applications, including the OS and application/software that are deployed and supplied by, and on, Sungard AS Managed AWS for UK Public Sector PaaS platform. Customer shall share the ITHC results with Sungard AS on request.

5. STORAGE SERVICES: MANAGED AWS FOR UK PUBLIC SECTOR

5.1. Storage Snapshots

Sungard AS will provide initial configuration of the snapshot frequencies and the retention periods for the number of VMs identified in the Order.

For the number of VMs identified in the Order, Sungard AS will provide:

(a) Changes to snapshot frequencies and retention periods via a chargeable service request.
(b) Machine or data restoration from a snapshot via a chargeable service request.

6. INCIDENT RESOLUTION SERVICES: MANAGED AWS FOR UK PUBLIC SECTOR

6.1. Eligibility

Incident Resolution Services shall be provided for those services or Sungard AS Equipment where Customer contracts for a hybrid or combined service that incorporates both AWS Infrastructure and Sungard AS Equipment, as specified in the Order. This service-level agreement (SLA) does not apply to any AWS Infrastructure.

6.2. Detection and Notification

Where Sungard AS detects an incident with eligible services or Sungard AS Equipment, Sungard AS will notify the Customer's Designees of the incident.

The Services use the criteria in the below table for prioritisation of incidents as defined in the Sungard AS Managed AWS for UK Public Sector contract.

Table 1. Managed AWS for Public Sector Incident Prioritization Criteria

Incident Priority	Contact Method	Criteria (Meets One or More)	Examples (Not a Definitive List)
P1	By phone only	Severely unusable. Severe disruption of service or business functions, possibly with revenue loss. Critical system failed or severely impaired. No workaround(s) exist. Affects critical business unit, users or functions.	Multiple server failures affecting key operational areas. Severe performance degradation. Financial systems affected in a short period. Security issue such as malware or virus.
P2	By phone only	Causes major business disruption. VIP user(s) or business unit with significant reduction in system performance. No workaround(s) exist. Potential to cause or become a P1 incident.	Slow response of key business application for one or more users. Security incident.
P3	By email or customer portal	Impacts system availability or service operation. Affects users within a single function. Workaround(s) may be in place. Business operations affected, but not severely.	Equipment failures that are covered by redundancy/resiliency. Server or infrastructure device identified as not having current patch/pattern files within 5 days of a patch being uploaded to the distribution servers by the service provider.
P4	By email or customer portal	Minor disruption or usability issues. Affects single user or function. Workaround(s) available. Does not affect business operations.	Incident queries relating to Data Center Services.

6.3. Time to Respond

Depending upon the categorization of the incident associated with the eligible item, then, within the corresponding timescale to respond from Sungard AS' detection or having been notified by Customer of the incident, Sungard AS will engage its then-available technical support personnel to assist (in conjunction with Customer's personnel) in incident diagnosis within the Service-Level Commitment detail in the Order. Customer also shall, as soon as reasonably possible, make available its personnel to assist in incident diagnosis.

Incidents are reported, responded to and resolved according to the Key Performance Indicator (KPI) specifications as shown below:

Table 2. Incident Response KPI Specifications

	Type	Service Level	Target	Measure
Response Time	KPI	Priority 1 (Critical)	15 minutes	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 2 (High)	30 minutes	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 3 (Medium)	60 minutes	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
	KPI	Priority 4 (Low)	2 hours	From the time the ticket is logged to the time it is electronically accepted by the resolving team.
Resolution Time	KPI	Priority 1 (Critical)	4 hours	For each Priority 1 (Critical) Incident, from the time the ticket is logged in the Ticket Management System to the time the Incident is resolved.
	KPI	Priority 2 (High)	8 hours	For each Priority 2 (High) Incident, from the time the ticket is logged in the Ticket Management System to the time the Incident is resolved.
	KPI	Priority 3 (Medium)	4 business days	For each Priority 3 (Medium) Incident, from the time the ticket is logged in the Ticket Management System to the time the Incident is resolved.
	KPI	Priority 4 (Low)	10 business days	For each Priority 4 (Low) Incident, from the time the ticket is logged in the Ticket Management System to the time the Incident is resolved.
Updates	KPI	Priority 1 Incident	Every hour (24x7)	A Sungard AS Service Desk incident assignee will contact Customer-named contact by phone every hour with an update on incident status.
	KPI	Priority 2 Incident	Every 2 hours (24x7)	A Sungard AS Service Desk incident assignee will contact Customer-named contact by phone every 2 hours with an update on incident status
	KPI	Priority 3 and 4	Every 24 hours, Monday to Friday	A Sungard AS Service Desk incident assignee will email Customer-named contact every 24 hours, Monday to

	Type	Service Level	Target	Measure
				Friday, with an update on incident status.
Reports	KPI	Priority 1 and 2	Within 4 business days of incident resolution	The Sungard AS Service Manager will create an incident report and present it to Customer Service owner.

6.4. Time to Fix

Sungard AS does not give any guarantee or warranty, nor is it a condition of the Order that Sungard AS will be able to fix any detected or notified incident with any eligible service or Sungard AS Equipment within any timescale because resolution will depend upon the nature and circumstances of the incident, Customer's timely assistance, and response times from Equipment and Software vendors. However, where Sungard AS can do so, it will use its reasonable endeavors to fix the incident as soon as possible and will otherwise liaise with the Equipment and Software vendors, Customer, and Customer's suppliers to enable them to do so. In addition, until resolution, Sungard AS will internally escalate the incident in its attempts to remedy the problem.

7. GENERAL SERVICE TERMS

These Services are also subject to the General Service Terms at https://www.sungardas.com/hubfs/_multimedia/document-file/sungardas-general-service-terms.pdf.