

**Appendix E to DIR Contract Number DIR-TSO-2736
CLOUD SERVICES CONTENT (ENTERPRISE CLOUD & PRIVATE CLOUD)**

Enterprise Cloud Resource Pool Services – Features

Sungard AS will provide the following in connection with the number of virtual machines (“VMs”) identified in the Order:

- The quantity of vCPU, RAM and storage, each as identified in the Order (collectively “Committed Cloud Resource Pool”);
- The use of additional vCPUs, RAM and storage (“Flex Resource Pool”), not to exceed 100% of the Committed Cloud Resource Pool, upon request pursuant to the terms of this Order (not applicable to Oracle Resource Pools);
- Load balancer infrastructure, configuration, implementation, configuration changes, patch management and installation, availability monitoring, incident management and problem resolution;
- Redundant firewall infrastructure, configuration, implementation, configuration changes, patch management and installation, availability monitoring, 10 site-to-site VPN tunnels, creation of backup and restore firewall rules, incident management and problem resolution; and
- In the case of Managed Cloud Services (Oracle Resource Pool), Software Licensing Services for the operating system identified in Part 1 of the Order and hosting of the VMs on multi-tenant servers used by multiple customers, unless identified as dedicated in Part 1 of the Order.

VMs may be used for “production purposes” (“Production VMs”) or pre-production purposes (“Pre-Production VMs”) as indicated on the Order. “Production purposes” means the VM is used by Customer solely in Customer’s enterprise production IT environment and not used in, including but not limited to, application testing, quality assurance, or development operations. Customer may not order Pre-Production VMs unless Customer has ordered or is operating at least one Production VM. Customer should contact their Account Executive to generate paperwork to convert any Pre-Production VM to a Production VM.

Private Cloud Resource Pool Services – Features

Sungard AS will provide the following in connection with the number of virtual machines (“VMs”) and primary and failover blades each as identified in the Order:

- The quantity of RAM and storage, each as identified in the Order (collectively “Committed Cloud Resource Pool”);
- Load balancer infrastructure, configuration, implementation, configuration changes, patch management and installation, availability monitoring, incident management and problem resolution; and
- Redundant firewall infrastructure, configuration, implementation, configuration changes, patch management and installation, availability monitoring, 10 site-to-site VPN tunnels, creation of backup and restore firewall rules, incident management and problem resolution.

VMs may be used for “production purposes” (“Production VMs”) or pre-production purposes (“Pre-Production VMs”) as indicated on the Order. “Production purposes” means the VM is used by Customer solely in Customer’s enterprise production IT environment and not used in, including but not limited to, application testing, quality assurance, or development operations. Customer may not order Pre-Production VMs unless Customer has ordered or is operating at least one Production VM. Customer should contact their Account Executive to generate paperwork to convert any Pre-Production VM to a Production VM.

Enterprise & Private Cloud Resource Pool Services – General

Sungard AS will notify Customer via email of the commencement of Customer’s access to the Cloud Services and provide credentials to log into its cloud environment (“Service Commencement Date”).

Customer may order additional Cloud Services and, in the case of Enterprise Cloud Services, Flex Resource Pool resources, which Sungard AS will provide at the rates identified in the Addenda attached hereto. Customer may contract for additional Cloud Resource Pool line items by executing a new Order. If Customer requests use of additional resources and does not execute a new Order, all such additional resources will be part of the Flex Resource Pool and will be invoiced at the rates identified in the Flex Resources Addendum until the earlier of (i) Customer’s request to remove the additional resources from the Flex Resource Pool, or (ii) the parties’ execution of a new Order adding the resources to the Committed Cloud Resource Pool. Customer may order additional Cloud Resource Pool items for Pre-

Production VMs, but may not order other Cloud Add-On Services for Pre-Production VMs unless such VMs are converted to Production VMs.

Customer may allocate and reallocate the VMs, vCPUs, RAM and storage quantities to 1 or more virtual datacenters at its discretion so long as the total quantity of each does not exceed the amount identified in the Order.

With respect to Enterprise Cloud Services, Customer use of the Flex Resource Pool will be invoiced in minimum 1 month increments until Customer requests, pursuant to the Customer Request Guidelines located in the Customer Portal, that Sungard AS terminate use of the Flex Resource Pool.

With respect to firewall infrastructure:

- Customer may request Sungard AS support for client VPN services of Customer-licensed client VPN software;
- Customer is responsible for software management and configuration of Customer-managed VPN site-to-site end-point(s); and
- Sungard AS does not monitor VPN persistence.

Sungard AS maintains exclusive control of system administration security (e.g., administrator or root) level access for firewall and load balancing infrastructure.

Managed Internet Access Services: Cloud – Features

Sungard AS will provide the amount of bandwidth on the Order and, for Sungard AS-provided IP addresses, will provide the following, in accordance with the Customer completed design requirements form:

- IP Address registration;
- Registered Autonomous System Number (ASN) (only applicable for Customers who require BGP peering);
- Monthly report of bandwidth utilization;
- Up to 5 DNS changes with up to 10 records per change per month, for Customer-registered domain names; and
- Domain name administration services for up to 10 primary and/or secondary Customer domain(s).

Managed Internet Access Services: Cloud – General

Sungard AS assigns IP addresses in accordance with the requirements of American Registry for Internet Numbers (ARIN) and Réseaux IP Européens or European IP Networks (RIPE). If Customer has significant IP requirements (for example, in excess of 1,000 public IP addresses), Sungard AS may require that Customer contact ARIN directly to register the IP addresses.

Network addresses assigned from Sungard AS are non-portable. Network space allocated to Customer by Sungard AS must be returned to Sungard AS in the event the Managed Internet Access Services are terminated or cancelled.

Production and Pre-Production VM Services: Cloud – Features

Sungard AS will provide the following for the number of VMs (Production and Pre-Production) identified in the Order:

- Initial operating system build, agent installation (if applicable).

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

- Operating system level backups configuration in accordance with the Customer completed design requirements form;
- Operating system configuration changes upon Customer request;
- Management of system administration security access (e.g., root or administrator access);
- Installation of antivirus software on Windows operating system servers;
- Administration of up to 10 Active Directory and/or LDAP accounts;
- Monitoring operating system patch alerts and providing Customer notification of such patches;
- Execution of daily backup schedules, retention of backup data for 4 weeks, weekly off-site rotation of media, file restore from media upon Customer request; and modification(s) to the backup schedule upon Customer request, 1 initial data restoration test;

- Operating system problem resolution and incident management; and
- Monitoring of availability & thresholds identified in Customer-completed design requirements form and Customer notification if Sungard AS detects non-responsiveness or exceeded thresholds.

Production and Pre-Production VM Services: Cloud – General

This Service does not include the definition or the implementation of any database backup and/or restoration methodology.

For all Production VMs receiving Operating System Management Services: Cloud, Customer will:

- Provide verification of licenses and necessary license keys applicable to Customer-provided software prior to Service provision by Sungard AS;
- Provide Sungard AS system administration security (e.g., administrator or root) level access for each VM and, if Customer retains system administration security access level access, permit such access to be traced by Sungard AS; and
- Obtain and maintain 24x7 maintenance agreements with the original software vendor, for Customer-provided software and notify the vendor of Sungard AS' authorization to act as Customer's agent under the maintenance agreements.

Customer system administration access to firewall and load balancing infrastructure is not permitted.

Secondary Site Failover Services – Features

Sungard AS will:

- Failover the Managed Cloud and Managed Private Cloud Services (excluding Pre-Production VMs) to a secondary site if the primary Sungard AS site ("Primary Site") becomes unavailable in Sungard AS' sole reasonable discretion ("Failover Event"); and
- Provide up to 2 Customer tests of the Secondary Site Failover Services per 12 month period following the Order Service Commencement Date.

Notwithstanding the description above, if Customer has ordered Managed Oracle Services: Cloud, Sungard AS will provide the number of tests identified in Part 1 of the Order for the Managed Oracle Services: Cloud for the per test fee identified in Part 1.

Secondary Site Failover Services – General

Following a Failover Event, Sungard AS will notify Customer when the primary Sungard AS site is available and schedule with Customer the transfer of Customer data and applications back to the Primary Site no later than 14 days following the Customer's receipt of the Sungard AS notice of availability.

Customer tests of the Failover Services must be scheduled at least 30 days in advance pursuant to the Request Guidelines located in the Customer Portal.

Secondary Site Failover Services are available only where the Cloud Services are provided using infrastructure within a Sungard AS facility located in the U.S.

Failover Services for Private Cloud entail failover from a dedicated blade to an alternate dedicated blade.

Geographic Load Balancing Services: Cloud – Features

In connection with Production VMs identified on the Order (Pre-Production VMs are not supported), Sungard AS will provide the following for the number of load balancers identified in the Order located in multiple Sungard AS facilities, in accordance with the Customer completed design requirements form:

- Load balancer configuration, implementation and Customer-requested configuration changes;
- Installation of Customer-provided and maintained SSL certificates;
- Up to 5 DNS entries;

- Load balancer availability monitoring;
- Load balancer problem resolution and incident management; and
- Exclusive control of administrator security passwords and IDs (Customer may request a copy of device configuration data).

Host Intrusion Detection Services: Cloud (“IDS”) – Features

In connection with Production VMs identified on the Order (Pre-Production VMs are not supported), Sungard AS will provide the following for the number of VMs identified in the Order:

- Installation and configuration of IDS infrastructure in accordance with the Customer completed design requirements form;
- Configuration of IDS rules, including fine tuning of rules during 30 day period following initial configuration and implementation of Customer-requested changes to IDS rules;
- Automatic implementation of new attack signatures as made available by vendor;
- 24x7x365 intrusion monitoring and notification to Customer of detected alerts based upon manufacturer and Customer approved settings; and
- Retention of IDS logs for 90 days.

Host Intrusion Detection Services: Cloud (“IDS”) – General

Customer administrative access to Sungard AS devices used to provide IDS is not permitted. Customer may request a hardcopy or electronic copy of device configuration data.

Threat Manager Services: Cloud – Features

Sungard AS will provide the following in accordance with the Customer completed design requirements form for the number of Customer-specified nodes identified on the Order:

- Monitoring, analysis and logging of security events;
- Sensor tuning and optimization;
- Threat and vulnerability signature updates;
- Asset identification and criticality ranking;
- Vulnerability assessments and related reporting;
- Web portal access;
- Customer-selected notification of detected threats via email or page as identified in the Customer completed design requirements form; and
- Intrusion Detection Services.

If identified on the Order, Sungard AS will provide the Threat Manager - SSL Decryption Service which enables the Threat Manager Service to decrypt and inspect SSL encrypted network traffic to identify potential security threats.

If identified on the Order, Sungard AS will provide the Threat Manager - Active Watch Service which provides access to SANS GIAC certified Intrusion Detection analysts who analyze data that is generated through the Threat Manager Service. Customer will be alerted when valid hostile traffic is identified and will be advised on potential remediation steps. Security Analysts monitor the network on a 24/7/365 basis.

Log Manager Services: Cloud – Features

Sungard AS will provide the following for the number of Customer-specified log sources identified in the Order:

- Collection, storage, reporting and correlation of log data;
- Storage of log data for 1 year unless otherwise specified in the Order;
- Threat and vulnerability signature updates; and
- Web portal access.

If identified on the Order, Sungard AS will provide the Log Manager - Log Review Service which provides analyst review of the previous day's log data collected and stored by the Log Manager Service in order to identify and notify Customer of potential security incidents and to document such incidents and related actions taken.

Threat Manager and Log Manager Services: Cloud – General

The Threat Manager and Log Manager Services are provided using a third party subcontractor.

Software Licensing Services – Features

In connection with Production VMs identified on the Order (Pre-Production VMs are not supported), Sungard AS will provide, install and configure the number and type of software packages identified in the Order and access to the software vendor for maintenance and support through Sungard AS' maintenance agreement covering the software packages.

Software Licensing Services – General

Customer will comply with the third party vendor licensing terms and conditions applicable to the software package.

Upon termination of the Software Licensing Services, Customer will de-install and immediately discontinue all use of the software provided under Software Licensing Services.

BlackBerry® Enterprise Server Services: Cloud – Features

In connection with Production VMs identified on the Order (Pre-Production VMs are not supported), Sungard AS will provide the following for number of BlackBerry Enterprise Server Accounts ("Accounts") hosted on the VMs, each identified on the Order:

- Remote provisioning of Accounts based on the Customer-completed design requirements form;
- Re-provisioning of existing Accounts to reset passwords or associate with new mobile devices; and
- Routing email between Customer's Exchange environment managed by Sungard AS and those Customer selected mobile devices associated with email addresses hosted in such environment.

BlackBerry Enterprise Server Services: Cloud – General

Customer will:

- Provide Sungard AS with information necessary for provisioning of the Service, including PIN number's associated with the mobile devices;
- Purchase and maintenance of all handheld BlackBerry mobile devices;
- Contract with a mobile services carrier supporting the transport of email using the RIM® BlackBerry network; and
- License, install and maintain BlackBerry desktop software on Customer equipment

Remote provisioning of Accounts may result in interruption of the Hosted BlackBerry Services for up to 24 hours.

Customer will comply with the third party vendor licensing terms and conditions applicable to the software package.

All application functional testing and validation is the responsibility of the Customer.



GENERAL CLOUD SERVICE CONDITIONS

Monitoring is conducted at 5 minute intervals. Customer notification is triggered by 2 consecutive negative polling responses.

Monitoring detects only positive or negative ICMP/SNMP responses from direct NIC polling and does not detect SNMP traps. Monitored devices may generate false-positive alerts that are caused by network congestion or application activity.

The monitoring components of the Cloud Services may require a monitoring agent be installed on the operating system. Customer will install the agent and vendor required upgrades or updates, unless the operating system is managed by Sungard AS.

In the event there is more than one instance or partition of an operating system or application running on a monitored device, then the Sungard AS monitoring "unit" is per instance instead of per VM.

Sungard AS' standard daily backup window begins at 6PM in the time zone where the Protected Servers are located and ends at 6AM in the same time zone the following day. Sungard AS cannot guarantee that backups will be completed within scheduled backup window(s) or that data restoration will occur within a defined period of time as both are dependent on the quantity of data to transfer and network bandwidth availability.

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

Database licenses are provided by Customer unless included in the Order under Software Licensing Services.

Sungard AS does not guarantee a time to fix Customer-provided software. Sungard AS will engage and manage vendors in accordance with the terms of the underlying maintenance agreement and is not responsible for vendor failures.

Sungard AS will provide technical support, problem resolution and change management for Production VMs in accordance its Support and Change Management Policy located in the Customer Portal.

Upon the expiration/cancellation of the Order for any reason, Customer will delete or migrate all Customer data resident on Sungard AS systems or equipment. To the extent that Customer fails to do so, Sungard AS will delete all such Customer data and software.

SERVICE LEVEL AGREEMENT (“SLA”)

Cloud Availability									
<p>Agreement. Each Cloud Production VM will be available for Customer use 99.95%. A VM is deemed available if it is responsive to 5 minute interval standard ICMP or SNMP requests AS shall measure the requests on a monthly basis and compute the number of failed requests as a percentage of the total number of requests.</p>									
<p>Remedy. If Sungard AS fails to meet the Cloud Availability SLA, Customer is entitled to a credit equal to the percentages identified in the table below for each month in which the failure occurred:</p> <table border="1"> <thead> <tr> <th><i>Cloud Availability Percentage</i></th> <th><i>Service Credit (% of pro rata portion of the Order's Monthly Fee based on VMs affected)</i></th> </tr> </thead> <tbody> <tr> <td>≥99.9% and <99.95%</td> <td>10%</td> </tr> <tr> <td>≥99.5% and <99.9%</td> <td>20%</td> </tr> <tr> <td><99.5%</td> <td>30%</td> </tr> </tbody> </table>		<i>Cloud Availability Percentage</i>	<i>Service Credit (% of pro rata portion of the Order's Monthly Fee based on VMs affected)</i>	≥99.9% and <99.95%	10%	≥99.5% and <99.9%	20%	<99.5%	30%
<i>Cloud Availability Percentage</i>	<i>Service Credit (% of pro rata portion of the Order's Monthly Fee based on VMs affected)</i>								
≥99.9% and <99.95%	10%								
≥99.5% and <99.9%	20%								
<99.5%	30%								
Cloud Secondary Site Failover									
<p>Agreement. For all Managed Cloud Services for which Customer has conducted a Failover Services test within the previous 6 months, Sungard AS will meet a 30 minute recovery point objective and 4 hour recovery time objective (respectively “RPO” and “RTO”), if Sungard AS uses the Cloud Secondary Site Failover Services to transfer the applicable Cloud Services to a secondary Sungard AS site, measured from the time of Sungard AS’ determination of the need for a Failover Event until Sungard AS begins provision of the Cloud Secondary Site Failover Services.</p>									
<p>Remedy. If Sungard AS fails to meet the Cloud Secondary Site Failover SLA, Customer is entitled to a credit equal to the percentages identified in the table below for each month in which the failure occurred:</p> <table border="1"> <thead> <tr> <th><i>RPO or RTO actual time</i></th> <th><i>Service Credit (% of Order's Secondary Site Failover Monthly Fee)</i></th> </tr> </thead> <tbody> <tr> <td>RPO = 45min - 60min / RTO = 6hr - 8hr</td> <td>25%</td> </tr> <tr> <td>RPO = 60+min - 120min / RTO = 8+hr - 12hr</td> <td>50%</td> </tr> <tr> <td>RPO = 120+min / RTO = 12+hr</td> <td>100%</td> </tr> </tbody> </table>		<i>RPO or RTO actual time</i>	<i>Service Credit (% of Order's Secondary Site Failover Monthly Fee)</i>	RPO = 45min - 60min / RTO = 6hr - 8hr	25%	RPO = 60+min - 120min / RTO = 8+hr - 12hr	50%	RPO = 120+min / RTO = 12+hr	100%
<i>RPO or RTO actual time</i>	<i>Service Credit (% of Order's Secondary Site Failover Monthly Fee)</i>								
RPO = 45min - 60min / RTO = 6hr - 8hr	25%								
RPO = 60+min - 120min / RTO = 8+hr - 12hr	50%								
RPO = 120+min / RTO = 12+hr	100%								
SLAs General									
<p>If Sungard AS fails to meet the same SLA 3 times within any 12 month period, as Customer’s sole remedy (in addition to any credits previously issued), Customer may terminate the Order by providing Sungard AS advance written notice no later than 60 days following the third SLA failure.</p>									
<p>If Sungard AS fails to meet an SLA, Customer is entitled to receive the applicable credit as Customer’s sole monetary remedy.</p>									
<p>In no event will the total credits for all occurrences during a month exceed the Order’s then current Monthly Fee.</p>									
<p>Credits and termination rights accrue solely with respect to the root or primary SLA failure and not for SLA failures that occur as a result of a root or primary SLA failure.</p>									
<p>Sungard AS will not be responsible for the failure to meet an SLA if the failure is caused by:</p> <ul style="list-style-type: none"> • A breach of the Master Agreement by Customer, its employees, subcontractors or agents (“Customer Representatives”); • The negligence or intentional acts or omissions of Customer or Customer Representatives (including Customer retention of root or admin access and changes to data or configurations); • Scheduled maintenance (including upgrades, repair or component replacement or scheduled backups) or other mutually agreed-to downtime; • In the case of Cloud Services, the absence of a patch, repair, policy, configuration or maintenance change recommended by Sungard AS but not approved by Customer, or configurations or architectures that are not supported or recommended by the applicable vendor; or 									

- Except in the case of Cloud Services, equipment malfunction (provided said equipment has been maintained by Sungard AS in accordance with the terms of the Agreement), scheduled maintenance (including upgrades, repair or component replacement or scheduled backups) or other mutually agreed-to downtime, or the failure of any software to perform in accordance with its specifications (“Software Failure”) and such Software Failure is not caused by Sungard AS’ negligence, willful misconduct or failure to maintain a maintenance contract on such software. In the event of a Software Failure, if in the reasonable discretion of Sungard AS and Customer, such Software Failure cannot be corrected, Customer may terminate the Order without penalty, upon written notice to Sungard AS.

ECS0314