Appendix E

to DIR Contract Number DIR-TSO-3083

Dell Cloud Dedicated

Service description | February 2014

Introduction

Dell Cloud Dedicated (the "Service") is an infrastructure as a service (IaaS) offering designed to provide a secure private cloud environment, hosted and managed by Dell, consisting of specific units of Dell x86 processing, power, storage and memory capacity. This Service Description and the attached appendices (collectively, the "Service Description") describe the Service being provided to you ("Customer" or "you").

The scope of this service

Many organizations wanting to host sensitive data or high performance applications with a cloud provider require architectural options that are not available from standard, public, multi-tenant cloud services. This Service offers more flexibility than public cloud by enhancing the Customer’s ability to operate production workloads, which might otherwise be limited to custom, on-premise operations, in a hosted private cloud.

Table of contents

Service details and options

Service details – general

Account setup	One-time fee. Amount variable depending upon size of environment.
Server blade with 2 CPU socket, 8 or 6 CPU core (depends on availability) 256 GB or 192 GB memory; minimum of two blades configured for high-availability. Available in fiber channel or iSCSI.	Included
Microsoft Windows server operating system for each host	Required for hosts running Windows VMs. Not required for Linux.
VMWare dedicated vCenter	Included
VMWare cluster	Included
Storage: Recommended non-tiered as minimum 80GB boot drive with 150GB data store per virtual machine ("VM")	Recommended minimum sizing
Dell SecureWorks infrastructure security monitoring	Included
24x7x365 technical support	Included
Dell Infrastructure hardware monitoring	Included
Service management support of the service	Included
Microsoft SQL server database	Optional

Service details – network options

Internet - full service committed bandwidth Service provides committed bandwidth that is reserved for the customer's consumption. Full service also allows customers to leverage Dell F5 load balancing features for virtual servers.	Optional. Additional setup fees will apply for servers being added to the F5 load balancer.
Internet – committed bandwidth only Service provides committed bandwidth that is reserved for the customer's consumption. Load balancing is not available with this service.	
Internet - burst Bursting capabilities allow customers to account for that extra level of bandwidth needed to accommodate peak demand without performance degradation (see Appendix G for additional details)	
VPN Managed VPN services providing site-to-site connectivity	Optional
MPLS Minimum 2MB connection from Dell to either ATT, Verizon or Level 3 MPLS Cloud (Customer is responsible for establishing connectivity on their side) (see Appendix H for additional details)	
Managed firewall service managed firewall service to enable proper configuration of firewall settings	Required in all cases A

Service details – storage options

Non-tiered (10Gbe iSCSI storage) • Normal – typical general server use (7.2k rpm) • High – high reads/writes: databases (15k rpm)	Optional
Tiered (block storage) High tiered performance storage that can move data from normal to high speed based on usage (read/writes). Auto selects the performance for the customer without intervention. Multiple storage types to ensure best performance.	Optional
NFS Ability for the customer to manage the storage directly at the VM level. Can be shared across VMs / clusters / etc.	Optional
Dedicated array For those customers that require an entire storage array dedicated to their environment, Dell offers two options. These are NOT usage based as the customer will be consuming the entire array. Customer will be billed monthly for the entire array regardless of the amount consumed. • Dedicated SAS array 9TB capacity • Dedicated SATA array 14TB capacity	Optional

Service details – compliance options

HIPAA and HITECH The Dell cloud dedicated environment has been designed to meet the security standards set forth by the HIPAA and HITECH security guidelines. (See Appendix E for additional details)	Optional

Service details – above the hypervisor managed services options

Cloud Colocation services Provides secure, rack space for the hosting of rack mountable servers/devices in the Plano Technology Center. Racks are preconfigured to cross connect Dell cloud to allow for network connectivity between the customer's servers/devices and customer's cloud environment. Rack space is sold in minimum increments of 5 Rack Units. Charges apply for racking, stacking and cabling as well as moves, adds, changes and deletes. (See Appendix I for additional details)	Optional
OS management Available for those customers that prefer to have Dell manage their virtual operating systems within the customer's cloud environment. This service is offered in tiers depending on the level of management that the customer desires. (See Appendix J for additional details)	Optional

Service details – other available services

Provides a cloud based integration toolset enabling integration between the customers' on premise applications, cloud based applications and SaaS provider applications.	Available upon request. Inquire with your sales representative.
SecureWorks managed security services Vulnerability management service ("VMS") Analyzes guest OSs and applications for security weaknesses; provides guidance on how to remediate. Dell SecureWorks will run scans, set up scheduled scans, and help customers manage the results. This service includes automated updates and deploys in minutes. Customers self-deploy a virtual scanning appliance into a VM in their virtual datacenter. Web application scanning service Analyzes web applications (internal and external) for security weaknesses; provides guidance on how to remediate. Dell SecureWorks will run scans, set up scheduled scans, and help	Available upon request. Inquire with your sales representative.

customers manage the results. Includes automated updates and is deployed quickly in the same manner as VMS.

Global threat intelligence service

Delivers continuous updates about threat landscape and emerging attack methods. Requires no time to deploy. Dell SecureWorks enables this feed in the customer portal upon service activation.

Billing and contract obligations

Your order form will list the service options you have purchased. If purchased, such service options form part of your Service.

Purchase Orders, Invoices and Payments shall be in accordance with Section 7 of Appendix A, DIR Contract Number DIR-SDD-1951. Billing for the Service is performed on a monthly basis in arrears and will include both fixed and variable costs. Capacity additions (for example, adding an additional blade or adding VM profiles) added within the last 7 days of the month will not be charged for the month in which the capacity is added. Customer will be charged the full amount starting the next month. Capacity additions added prior to the last 7 days of the month will be charged the full, non-prorated rate for the month in which the capacity was added.

The Service is offered with a minimum one (1) year contract. At the end of the contract, the Customer will automatically be renewed for another year unless sufficient written notice (30 days) is provided to the contrary to your account representative. Customer may choose to move to a month-to-month subscription after the first year is complete.

For billing-related questions, call toll-free at 1-866-712-3246 from the United States (option #3) M-F, 8AM-5PM (Central).

Guest operating systems

You may use a Dell virtual machine template or import your own OS image. The current list of VMware vSphere supported guest operating systems can be found here: http://www.vmware.com/pdf/GuestOS_guide.pdf. Customer is responsible for obtaining software license rights for any software used in connection with the Service other than software provided by Dell.

Dell virtual machine templates	
Microsoft Windows Server 2003 or 2008 (32-bit or 64-bit)	Included
Microsoft Windows Server 2003 or 2008 (32-bit or 64-bit) + SQL Server Standard	Included
Microsoft Windows Server 2003 or 2008 (32-bit or 64-bit) + SQL Server Enterprise	Included
SQL Enterprise Server 2008 R2 (64-bit)	Included
Red Hat Enterprise Linux (32-bit or 64 bit)	Included
CentOS Linux	Included
Ubuntu Server	Included

Networking

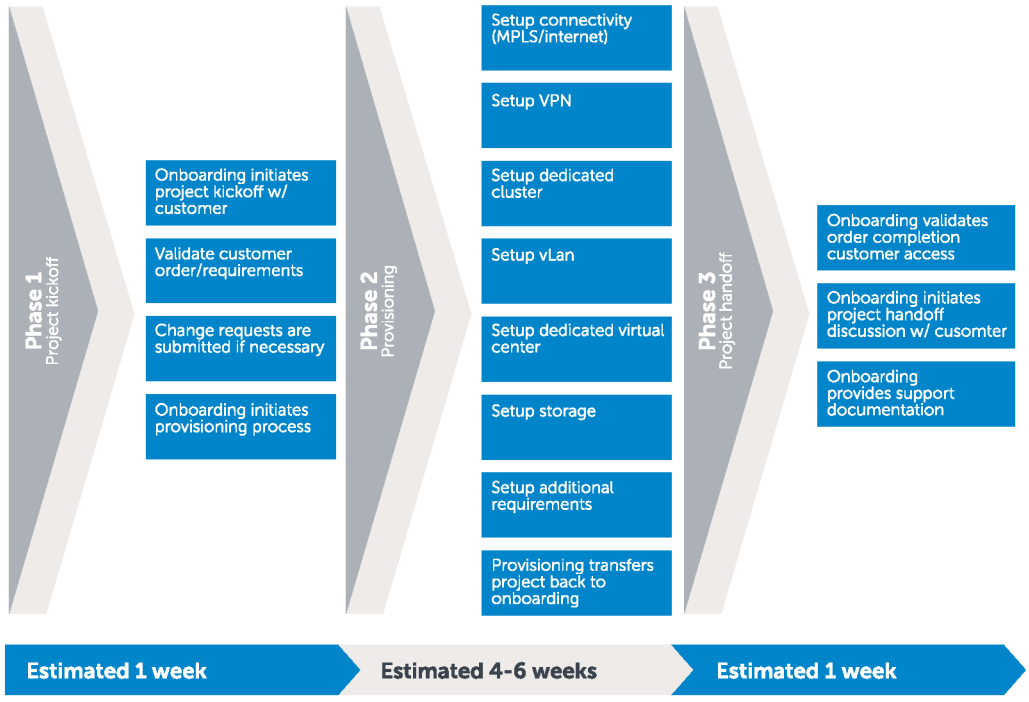
The networking portion of this Service consists of physical and virtual components. You will be provided a minimum bandwidth of 1MB with optional burst capabilities available. If you purchase Full Service Committed Bandwidth, load balancing and monthly reporting are included (see Appendix G for additional details). Customer may purchase the Dell optional Leveraged MPLS Service which allows Customer to connect to the Dell datacenter over an Extranet VPN (see Appendix H for additional details).

Data bandwidth in and data between VMs in the same datacenter will not be charged. Dell is responsible for operating, maintaining, and troubleshooting all physical network components residing in Dell data centers. Customer is responsible for operating, maintaining and troubleshooting all virtual networking components created in its virtual environments.

Backup and recovery

Dell performs daily snapshots of all storage arrays and maintains copies for a rolling 7 day period; this is included in the standard offering at no additional charge. For an additional charge, an optional backup service is also available where Dell will perform daily backups on a rolling 7 day schedule and retain weekly backups on a rolling 6 month schedule. Backup is done at a VM level (selection of individual files is not supported). This is a custom service that will need to be discussed with your account rep for further pricing.

Onboarding process



The Dell Global Onboarding Team will collaborate with designated Customer contacts to provide standardized onboarding of the Service ("Onboarding"). A high-level over view of the Onboarding process is set forth above. Following the Activation Date an assigned Dell representative will contact Customer to enable Onboarding, which will include:

- A phased project management process with defined project deliverables (kick off, provisioning, validation testing, training)
- Customer designation of authorized persons who are entitled to make Service-related requests
- An assigned Dell Project Manager and Technical Consultant for the duration of Onboarding
- Provisioning ("Provisioning") is considered complete when Customer is capable of accessing and operating the vCenter console
- Creation of and troubleshooting of one or more of the Customer's dedicated vCenter environment(s)
- Enabling administrator rights to your dedicated vCenter for holistic management of your environment
- Providing Customer virtual access to its dedicated vCenter
- If applicable, work with Customer to set up any optional services Customer has purchased
- Providing Customer access to its Dell Portal
- A 1 hour Customer walk-through training session on its vCenter and dedicated resources
- Transition to Dell Support

The activation date ("Activation Date") of this Service Description is the date on which the related Order Form is executed by the Customer and accepted by Dell. Billing will begin at the conclusion of Provisioning (the "Billing Start Date").

Support

You may contact Dell support via phone 24x7x365. Support may be provided from outside of the country or region in which Customer or Customer's end users reside. Support is provided in English only.

Customer responsibilities

- Customer will support Onboarding activities set forth herein for the Service. Customer will obtain all licenses necessary in connection with all software and applications used for the Service other than software provided by Dell.
- Customer will provide timely access to Customer resources, including but not limited to, virtualization administrators and engineering and project management. Dell and the Customer to agree on standard access protocols.
- The Customer is responsible for modifying and tracking changes to its dedicated virtual application environment.
- With respect to access to vCenter, the rename (configured) items will not be provided to Customer and Customer agrees to only self-provision from approved templates.
- It is the Customer's responsibility to perform complete backups of all existing data, software, and programs. The Dell backup responsibility is limited to performing daily snapshots and, if purchased, providing backup and recovery services as described above. NOTWITHSTANDING ANYTHING CONTAINED HEREIN TO THE CONTRARY OR DELL'S PERFORMANCE OF BASIC SNAPSHOT SERVICES OR BACKUP AND RECOVERY SERVICES, DELL WILL HAVE NO LIABILITY FOR LOSS OR RECOVERY OF DATA OR PROGRAMS or loss of use of system(s) arising out of the Service or support or any act or omission, including negligence, by Dell or a third-party service provider.
- Customer is responsible for all design and implementation of network security settings and requirements definitions.
- Customer is responsible for all application development and management and performance monitoring and all database development and management.
- Customer is responsible for managing its virtual environment.
- Customer is responsible for any changes/modifications/deletions to Customer's virtual environment.
- Customer is responsible for providing security management and access control for in-service x86 Virtual Servers, including Customer software and data.

Toll-free from the United States:

1-866-712-3246

Option **#2** for Dell cloud dedicated service technical support (24x7x365)

When contacting support for Dell cloud dedicated service

- A support desk agent will create a service request
- The request will be provided to the appropriate service organization and a specialist will follow up with you
- The incident number will be supplied for reference when speaking with the support specialist and for future follow-up

Dell support responsibilities

- Assist Customer in identifying causes of issues experienced in Customer's virtual environment
- Assist in troubleshooting the Customer's vCenter environment
- Assist in creating, modifying, copying VMs, if necessary
- Assist in decommissioning VMs
- Support backup/recovery requests, which may include additional costs and be subject to a separate agreement
- Work with Customer to troubleshoot any dedicated VPN links over the Internet or dedicated WAN links
- Answer questions related to billing and invoices
- Provision new infrastructure, for example, blades, storage, firewalls, routers, etc.
- Perform routine maintenance and patching on the infrastructure
- Perform incident management
- Perform the following functions with respect to the Dell private cloud as they as they relate to:
  - Hypervisor: manage and maintain vCenter, perform setup and configuration of the hypervisor and patch the VMware environment
  - Hardware: manage and maintain servers, storage (RAID Protected), networking infrastructure (leveraged VPN/MPLS/ Internet) and perform hardware administration
  - Facilities: manage and maintain Dell data center(s), racks, power, cooling and security

Reporting

Upon request, Dell will provide the reports listed on Appendix D (Reporting).

Miscellaneous

The following will apply if Customer is located in Canada: The Services may be provided from locations outside of Canada. In no event will Dell be responsible or liable for determining whether Customer is permitted to transmit, disclose, transfer, host or make available any data provided or transferred to, or accessed or hosted by Dell from any location outside of Canada. All such responsibilities for making such determination remain and reside with Customer and any risk for any failures of Customer to adhere to applicable privacy and data protection laws by transferring or disclosing data to Dell hereunder will remain exclusively with Customer. Customer will be responsible for obtaining any third party rights, permissions and consents or providing any notices to third parties as may be required in respect of the above. Customer represents and warrants that it has obtained all rights, permissions, and consents necessary for Dell to obtain, access, process, host, transfer, or otherwise use, as applicable, any Customer provided or accessible data in accordance with this Agreement, including, without limitation, all applicable or necessary rights, permissions and consents.

This Service Description does not confer on Customer any warranties which are in addition to the warranties provided under the terms of your master services agreement or Agreement, as applicable.

No hardware or software is being transferred, sold, leased or licensed to the Customer under this Service Description. Dell uses hardware or software as part of its delivery of the Service; other than in connection with Cloud Colocation Services, such hardware or software is licensed, owned or otherwise held by Dell.

To the extent applicable, Customer agrees that the Dell privacy and security requirements satisfy any and all obligations under the Family Educational Rights and Privacy Act, 20 USC 1232g, and its implementing regulations, 34 CFR pt. 99 (collectively, "FERPA") that Dell may have as a recipient of education records and personally identifiable information contained in such records.

Dell will provide security in connection with the Service in accordance with the Security Statement attached as Appendix C.
The excluded support/services described below are available from Dell outside of this Service Description for an additional charge.

- Virtualization design
- Evaluation of Customer's IT operations and organization
- Migration of any existing physical servers into a virtualized server environment
- Virtualization platform software licenses in Customer's data center
- Application profiling, which includes identification of applications compatible with virtualization and analysis of server/ application interdependencies, and
- Any activities other than those specifically noted in this Service Description

Terms & Conditions

Appendix A:

Service level agreement for Dell Cloud Dedicated

The service levels and associated remedies described below apply to the Service when that Service is purchased directly from Dell.

Availability SLA
During the term of the applicable Order Form between Dell and Customer for the Service and following the Billing Start Date, Dell will use commercially reasonable efforts to achieve 99.95% Availability for the Service infrastructure for any calendar month. If we do not meet this Availability SLA (the "Availability SLA"), and so long as your account with Dell is current and not suspended, you may be eligible to receive Availability Credits (defined below). Dell will use reasonably suitable monitoring tools to collect production server, storage and network uptime data. Dell reserves the right to schedule reasonable weekly maintenance windows ("Maintenance Windows") during which time Dell will perform repairs or maintenance or remotely patch or upgrade software.

Definitions: The following definitions apply to this Availability SLA.

"Availability" means Uptime divided by Scheduled Uptime multiplied by 100%. Availability is determined per the Monthly System Availability Reports. Availability is rounded to the nearest two-tenths of one percent.

"Exceptions and Exclusions" means (i) outages that occur during Maintenance Windows or during emergency maintenance windows (ii) outages attributable to a network carrier, (iii) failures attributable to the Customer's network, (iv) failures that result from changes to network circuits from Customer location(s) to Dell facilities that result in reduced bandwidth capacity for the Service, (v) failures attributable to a force majeure event, (vi) failures attributable to a breach of this Service Description by Customer, (vii) failures attributable to the acts or omissions of the Customer, a vendor or an entity to which Services are provided, (viii) Customer exceeds 85% of virtual server cluster capacity, or (ix) total used storage exceeds 85% of purchased storage. Dell will notify Customer when total used storage reaches 75% of purchased storage. Should total used storage exceed 85% of purchased storage, Dell will not be liable for any failure to satisfy an Availability SLA target until total used storage returns to less than 85% of purchased storage.

"Scheduled Uptime" means the total number of minutes within any whole month minus the number of minutes set aside for scheduled maintenance and upgrades multiplied by the Customer's virtual servers. For example, if Customer has 10 virtual servers, each of which is not expected to be available during a weekly four-hour maintenance window, the Scheduled Uptime for the Service for that particular week would be 98,400 minutes: [10 virtual servers * ((60 minutes * 24 hours * 7 days) – (60 minutes * 4 hours * 4 weeks))]. If the actual Uptime for these 10 virtual servers during a month (in this case a month with 28 days) is 392,850, Availability for that month would be 99.8% (392,850 minutes divided by 393,600 minutes multiplied by 100).

"Uptime" means the total number of minutes within any whole month that the Customer's virtual servers are available for use by the Customer. For clarity, Uptime will not be reduced as a result of any Exceptions and Exclusions. Dell uses active agent monitoring of hypervisor environment, and EKG active monitoring of cloud hosts. Additionally Dell performs syslog capture of all dedicated host events to further capture any timestamp information about lifecycle events

Service level credits: If Dell does not meet the Availability SLA for a particular month, Dell will, at Customer's request, provide the applicable remedy set out below ("Availability Credits").

Monthly availability	Availability credit
100% - 99.95%	0% of charges billed in month of occurrence
99.94% - 99.00%	1% of charges billed in month of occurrence
98.99% - 97.00%	2% of charges billed in month of occurrence
96.99% - 95.00%	3% of charges billed in month of occurrence
< 94.99%	4%of charges billed in month of occurrence

Example: If the monthly Availability was 99.80%, a 1% Availability Credit would apply toward the amount due for the month of occurrence.

Performance SLAs

During the term of the applicable Order Form between Dell and Customer for the Service and following the Billing Start Date, Dell will use commercially reasonably efforts to acknowledge and resolve Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents in accordance with the below-listed service levels (each a "Performance SLA," and together with the Availability SLA, the "SLAs"). If we do not meet a Performance SLA, and so long as your account with Dell is current and not suspended, you may be eligible to receive the below-listed performance credit (a "Performance Credit," and together with the Availability Credit, the "Credits"). Dell will use reasonably suitable monitoring tools to collect and report on Performance SLA data.

Definitions: The following definitions apply to these Performance SLAs.

"Measurement Period" means the time during, or frequency by which, a Performance SLA is measured.

"Reporting Period" means the periodic evaluation and reporting frequency for each individual Performance SLA.

"Resolution Time" means the elapsed time between (i) the moment a service ticket is opened in the Dell Service Management Workflow System, until (ii) the moment the service ticket is closed in accordance with the Dell procedures manual because (A) the incident is resolved and Customer has not provided an accurate notification to Dell that the incident has not been resolved; or (B) a temporary solution that addresses all of the material aspects of the incident (a "Workaround") is provided.

"Service Management Workflow System" means the request management workflow system that enables certain Customer-approved requestors to submit incident, systems change and request management workflows to Dell.

"Severity Level 1" shall mean any reported incident that has high visibility, materially impacts the ability to perform business operations, and for which there is no Workaround solution (for example, a network outage).

"Severity Level 1 Incident Acknowledgment Time" shall mean the elapsed time between submission of a Severity Level 1 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.

"Severity Level 2" shall mean any reported incident that has high visibility, materially impacts the ability to perform business operations. A Workaround is available, however, performance may be degraded or functions limited (for example, a router is down, however, traffic is re-routed with degraded performance).

"Severity Level 2 Incident Acknowledgment Time" shall mean the elapsed time between submission of a Severity Level 2 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.

"Severity Level 3" shall mean any single infrastructure component is moderately affected or completely inoperable. The incident typically has limited business impact (for example, a management blade is down, part of the database cluster is inoperable).

"Severity Level 3 Incident Acknowledgment Time" shall mean the elapsed time between submission of a Severity Level 3 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.

"Severity Level 4" shall mean any single infrastructure component is moderately affected or is partially inoperable or can continue to operate as long as a Workaround procedure is followed. The incident has limited business impact (for example, a customer report is formatted incorrectly).

"Severity Level 4 Incident Acknowledgment Time" shall mean the elapsed time between submission of a Severity Level 4 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.

Incident acknowledgement time SLA

Objective	Measures the aggregate acknowledgment time for Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents.

Method

Data capture	Incident records in the Service Management Workflow System are used to determine the total number of Severity Level 1, Severity Level 2, Severity 3 and Severity 4 incidents during a reporting period, the time each incident is received, and the elapsed time between submission of each Severity Level 1, Severity Level 2, Severity 3 and Severity 4 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.

Responsibility

Reporting period	Monthly
Management period	Monthly

Service metric

Values	Metrics: Severity Level 1 Incident Acknowledgement Time – fifteen (15) minutes Severity Level 2 Incident Acknowledgement Time – thirty (30) minutes Severity Level 3 Incident Acknowledgement Time – eight (8) business hours Severity Level 4 Incident Acknowledgement Time – thirty-six (36) business hours
Minimum service level	In the aggregate, 95% or more of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents are acknowledged within, respectively, the Severity Level 1 Incident Acknowledgement Time, the Severity Level 2 Incident Acknowledgement Time, the Severity Level 3 Incident Acknowledgement Time and the Severity Level 4 Incident Acknowledgement Time.
Other	If Dell fails to acknowledge an incident within the applicable minimum service level timeframe set forth above, but subsequently resolves such incident within the applicable minimum service level timeframe for incident resolution, Dell may exclude the incident from its calculation of the minimum service level.
Calculation	(Number of total Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents acknowledged, respectively, within the Severity Level 1 Incident Acknowledgement Time, the Severity Level 2 Incident Acknowledgement Time, the Severity Level 3 Incident Acknowledgement Time and the Severity Level 4 Incident Acknowledgement Time divided by the total number of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents) * 100
Performance credit	If Dell does not achieve the minimum service level, Customer will be entitled to a Performance Credit in the amount of 2% of the charges billed in the month of the occurrence.

Incident resolution time SLA

Objective	Measures the Dell resolution time for the resolution of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents.
Method	
Data capture	Incident tracking will be recorded and reported using Service Management Workflow System. Severity Level 1 and Severity Level 2 incidents are to be worked 24 hours a day, 7 days a week until Workaround or Services restoration is achieved.
Responsibility	
Reporting period	Monthly
Management period	Monthly
Service metric	
Values	Metrics: Resolution Time – Severity Level 1 – four (4) hours Resolution Time – Severity Level 2 – eight (8) hours Resolution Time – Severity Level 3 – three (3) business day(s) Resolution Time – Severity Level 4 – ten (10) business day(s)
Exclusions	Resolution Time does not include the time that incident management tickets are in "suspend mode" because of hand-off to Customer or Customer's vendors. Incidents determined to be within Customer's responsibility to resolve are excluded from the calculation.
Minimum service level	In the aggregate, 95% or more of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents are resolved within the applicable Resolution Times.
Calculation	(Number of total incidents at Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 closed within the applicable Resolution Time or properly downgraded by Dell to a lower Severity Level within the applicable Resolution Time, divided by number of the total incidents at Severity Levels 1, 2, 3 and 4) * 100
Performance credit	If Dell does not achieve the minimum service level, Customer will be entitled to a Performance Credit in the amount of 2% of the charges billed in the month of the occurrence.

Claim procures and credit limitations

Claim procedure: To receive a Credit, Customer is responsible for making a claim alleging Dell's failure to achieve the applicable SLA within 30 days of the last date of the reported downtime. The claim must be sent to the account Customer Executive or Delivery Manager. The claim must include the following information:

Customer's name; the name of the Service to which the claim relates (Dell Cloud Dedicated); name, e-mail address and telephone number of the appropriate Customer contact; the date(s) and times for each claim of downtime if claiming an Availability Credit; and the Performance SLA that was not achieved if claiming a Performance Credit.

Any “credit” that Dell may owe, such as a Performance Credit for a failure to meet an SLA, will be applied to rates due for the Service, and will not be paid as a refund. If a single Incident results in multiple acknowledgement time or resolution time defaults (as determined through the Dell root cause analysis), Customer shall receive only the highest Performance Level Credit applicable to such Incident. All claims for Credit are subject to review and verification by Dell, and all remedies will be based on Dell’s measurement of its performance of the applicable Service and decisions will be final. Customer’s sole remedy, and Dell’s sole liability, with respect to Dell’s inability to meet an SLA are the Credits described above and Customer explicitly disclaims any and all other remedies, whether in law or equity.

Appendix B:

Key performance indicators for Dell Cloud Dedicated

The Key Performance Indicators ("KPIs") described below are for measurement and reporting purposes only and apply to the Service when the Service is purchased directly from Dell. Any failure on the part of Dell to satisfy the below-listed KPIs will not entitle Customer to any credit or other remedy. Unless otherwise noted herein, the definitions set forth in Appendix A apply to this Appendix B.

Root cause analysis KPI

Objective	Report and track root cause analysis relating to the Dell infrastructure in accordance with the Dell problem management procedures.

Method

Data capture	Problem tracking will be recorded and reported using the Service Management Workflow System.

Responsibility

Reporting period	Monthly
Management period	Monthly

Service metric

Minimum service level	In the aggregate, 90% or more of Severity Level 1 incidents and Customer-requested Severity Level 2 incidents are subjected to a root cause analysis and are submitted to Customer for review within ten (10) business days of the later of (i) the Severity Level 1 incident moving to "Service Restored" status, or (ii) as to Severity Level 2 incidents only, Customer's request for a root cause analysis being entered in the Service Management Workflow System.
Calculation	(Number of Severity Level 1 and Severity Level 2 incidents subjected to a root cause analysis and submitted to Customer for review within the minimum service level divided by total number of Severity 1 incidents and Severity 2 incidents for which Customer requests a root cause analysis) * 100

Appendix C:

Dell Cloud Dedicated security statement

In the event of a conflict between the terms of this Appendix C and the applicable terms of the DIR contract, the terms of this Appendix C shall prevail for the purposes of these Services.

Commitment to security

The Service is designed and built to address key security aspects, including:

- Integrity: Through Internet Protocol Security (IPsec), Secure Shell (SSH) and Multiprotocol Label Switching (MPLS) connections, the Service provides industry standard encryption and message authentication to help ensure that customer data cannot be modified during transmission.
- Confidentiality: The Service is designed to allow only authorized users to access information in their virtual environment.
- Availability: The Service uses Uptime Institute Tier 3 or better data centers.

Overview

The Service uses the following controls so that the integrity, confidentiality and availability of your information meet strong industry standards:

- Physical controls: Including environmental controls, are countermeasures that affect the physical environment. Examples of physical controls include access controls, fire prevention systems, cooling systems, exit routes, security personnel and data center surveillance monitoring.
- Technical controls: Also called logical controls) are countermeasures that rely upon use of technology to mitigate risk; for example, firewalls, intrusion detection and prevention systems, and encryption mechanisms.
- Administrative controls: Countermeasures that involve policy and procedures; for example, security and escalation policies, log audits, vulnerability scanning and penetration testing.

Physical controls

Service data centers are designed to support and protect mission-critical operations. These data centers provide multi-level physical security features and a rigidly-controlled physical environment to help protect customer assets and operations. Service data centers are audited annually to the SSAE 16 Type 2 standard and maintain ISO/IEC 27001:2005 certification.
ISO/IEC 27001:2005 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system for managing an organization's information security risks. The Service with the applicable Dell data centers and supporting services are ISO/IEC 27001 certified: http://i.dell.com/sites/content/corporate/corp-comm/en/Documents/dell-plano-iso27001.pdf.

- Access and Security Controls: Access to Service data centers is highly controlled. All entrances are monitored and have alarms for protection. These data centers are staffed and patrolled by security officers 24x7 to augment physical security features, providing protection of your operations.
- CCTV Digital Recorders: CCTV security cameras monitor designated sensitive areas of the Service data center.
- Fire Suppression: Industry standard fire suppression systems for multi-tenant data centers are in use.
- Environmental Controls: Service data centers are constructed to meet high standards of redundancy. These data centers also include critical power and cooling systems that are provisioned with appropriate redundant failover infrastructure. The critical power and cooling infrastructure is backed up by an emergency power generation system.

Technical controls

- Network and System Security: Multiple levels of disparate defenses are used to protect customer information and to strictly control network access to the data center. Customers connect with the Service via IPsec, SSH and MPLS connections to provide industry-standard link encryption and message authentication to help prevent customer data from being modified during transmission. All access to Service servers is strictly monitored. In addition, Service servers are configured to prevent intrusions and protect against day-to-day threats. The servers are selected and configured to maximize their reliability, security, scalability and efficiency.
- Firewalls: Customer data transfers are made from the customer's environment to the Service system via standard Internet Protocol Security (IPsec), Secure Shell (SSH) or Multiprotocol Label Switching (MPLS) connections through the customer's firewall. All non-required firewall ports are blocked on the Service virtual firewalls.

- Intrusion Prevention Systems: Dell uses enterprise-grade intrusion detection / intrusion prevention systems (IDS/IPS) within the Service infrastructure to provide another mechanism for the early detection and prevention of data breaches.
- Security Operations Center Monitoring: All Service infrastructure components send system logs to a central log aggregation system. A dedicated Dell Security Operations Center (SOC) monitors the system logs, as well as firewall and IDS/IPS events 24x7 to facilitate early detection of any attempted data breaches. Dell SecureWorks provides this industry leading capability to provide reasonable assurance to customers that their infrastructure is safe, secure, confidential and available.
- Access Controls: Access to Dell corporate systems is restricted, based on procedures to ensure appropriate approvals. To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties and least privileges. Remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place. Specific event logs from key devices and systems are centrally collected and reported on an exception basis to facilitate incident response and forensic investigations by recognized experts in this area.
- Vulnerability Scanning and Penetration Testing: Internal and external vulnerability scans are performed on the Service infrastructure on a recurring basis. External and internal penetration tests, including network and application-layer penetration tests are performed annually. The customer is not authorized to perform their own penetration testing against the Dell infrastructure.

Administrative controls

- Data Center Access History: Physical access history to the data centers is recorded.
- Personnel Security: All users with access to the Service environment are responsible for compliance with Dell information security policies and standards. As part of the employment process, new employees undergo a screening process applicable per regional law. In the United States, personnel screening procedures include criminal background checks and drug screening.
- A banner stating the Dell standard on Acceptable Use is displayed upon login to servers, desktops and notebooks. Dell annual compliance training includes a requirement for employees to complete an online course and pass an assessment covering information security and data privacy. Additional mechanisms for security awareness and education include articles in the corporate newsletters, website and whitepapers, presentation seminars and additional online courses.
- Communications and Operations Management: Changes to the Dell-provided infrastructure and systems are managed by Dell through a centralized change management program, which includes testing, back out procedures, business impact analysis and management approval, where appropriate.

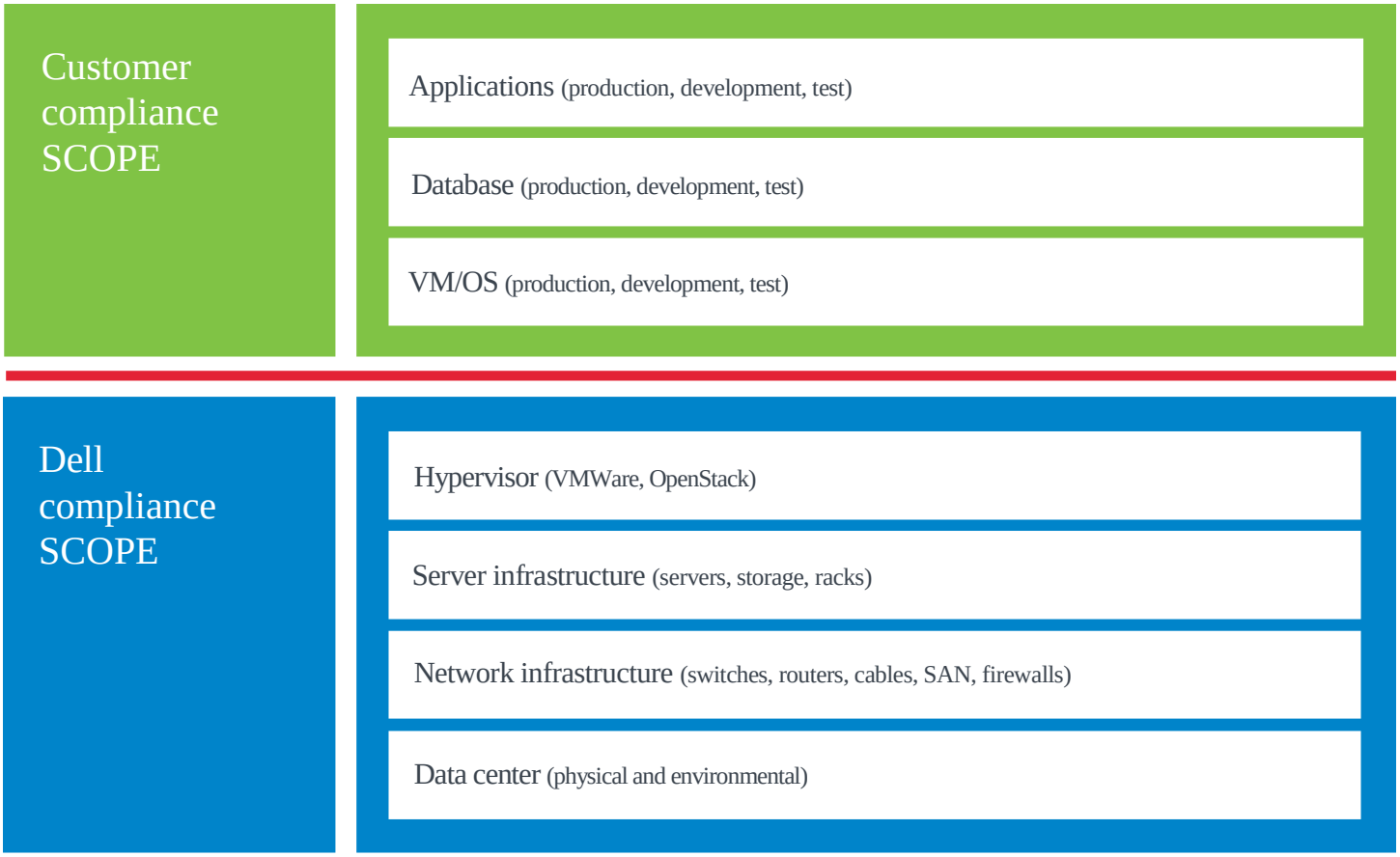
Incident response procedures exist for security and data protection incidents at the Dell-provided infrastructure level. The procedures include incident analysis, containment, response, remediation, reporting and procedures for returning to normal operations.

To minimize risk of malware infection, anti-malware software is used on all Service servers, as well as all desktop and notebook computers used by our personnel to connect to the Service infrastructure.

HIPAA & HITECH

The Service offers optional HIPAA- & HITECH- compliant security and privacy controls that enable healthcare-sector customers to host electronic protected health information (ePHI). Dell does not move Customer data between data centers unless such services are explicitly purchased; however, Dell proprietary information, including security logs and DCD monitoring and management information, may move between data centers and, will be kept in the continental United States.

Dell compliance responsibilities extend from the data center floor to the hypervisor. The Customer is responsible for their own compliance controls above the hypervisor, i.e. within the virtualized layer where the operating systems, databases, applications and integrations points reside. The below image illustrates this point.



Healthcare customers (i) see Appendix E which includes a HIPAA matrix that lists Dell's responsibilities versus the Customer's responsibilities, and (ii) are subject to the Business Associates Agreement set forth in Appendix E that outlines Dell's commitment to maintain the aforementioned compliance standards.

PCI customers see Appendix F for a PCI DSS Framework that provides a detailed explanation of the PCI DSS controls that Dell has implemented. The PCI DSS Framework also identifies any controls that remain exclusively the Customer's responsibility. In many cases, Dell and the Customer will be responsible for the identified control, but, as indicated above, Dell's responsibility ends at the hypervisor and Customer must manage these controls within the context of its DCD virtual data center environment.

If additional services are provisioned into the environment outside of the IaaS Services described in this Service Description, those additional services are responsible for supplying their respective security and compliance responses.

Appendix D:

Reporting

Service category	Report title	Frequency	Format	Comments
Utilization	Storage pools and volumes	Monthly	Excel	Data on storage provisioned and used for Customer VMs.
Utilization	VM machine inventory	Monthly	Excel	List of all Customer cloud VMs with associated ESX host names, DNS names, container names.
Utilization	Host inventory	Monthly	Excel	Listing of all customer ESX hosts (if applicable) and VMs located on each host.
Availability	Service level performance	Monthly	Excel	Service level performance for Customer's virtual environment availability.

Appendix E:

Business associate agreement for Dell Cloud Dedicated

In the event of a conflict between the terms of this Appendix E and the applicable terms of the DIR contract, the terms of this Appendix E shall prevail for the purposes of these Services. This Business Associate Agreement ("BAA") applies to the Service when that Service is purchased directly from Dell. Any capitalized terms used in this BAA that are not defined herein shall have the meaning ascribed to them in Health Insurance Portability and Accountability Act of 1996 as contained in 45 CFR parts 160, 162 and 164 ("HIPAA") and Subtitle D (Privacy) of Title XIII of Division A and Section 4104(b) of Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the "HITECH Act").

In order for Dell to provide the Service to Customer that requires access to Protected Health Information ("PHI"), Customer and Dell agree to the following terms related to the HIPAA privacy regulations contained in 45 C.F.R. parts 160 and 164 ("HIPAA Privacy Regulations"), the HIPAA security standards contained in 45 C.F.R. parts 160 and 164 ("HIPAA Security Regulations"), the HIPAA standards for electronic transactions contained in at 45 C.F.R. parts 160 and 162 ("HIPAA Transaction Regulations"), the HIPAA Breach Notification Rule as set forth in 45 C.F.R.Part 164 Subpart D, and the HITECH Act. This BAA shall commence on the Activation Date and shall automatically terminate on the expiration or termination of the Service.

- Permitted Uses and Disclosures: Dell is permitted to use and disclose PHI received or created by Dell from or on behalf of Customer as required to perform its obligations under the Service Description; provided, however, Dell may not use or further disclose PHI in a manner that would not be permissible if done by Customer, except Dell may also (a) use PHI for the proper management and administration of Dell or to carry out the legal responsibilities of Dell; (b) disclose PHI for the proper management and administration of Dell or to carry out the legal responsibilities of Dell if (i) the disclosure is required by law; or (ii) Dell obtains reasonable written assurances from the person to whom it disclosed the PHI that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Dell of any instances of which it is aware in which the confidentiality of the PHI has been breached; (c) use PHI to provide Data Aggregation services to Customer as permitted by 45 C.F.R. § 164.504(e)(2)(i)
(B) if the performance of Data Aggregation services is necessary for Dell to perform its obligations under the Service Description or Customer otherwise requests Data Aggregation services from Dell; (d) use and disclose PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1); and (e) use and disclose PHI as required by law.

- Subcontractors and Agents: Dell may disclose PHI to its agents, subcontractors and representatives solely for those purposes set forth in Section 1 of this BAA only if such agents, subcontractors and representatives agree in writing to be bound by and comply with restrictions and conditions that are substantially similar in all material respects to the restrictions and conditions regarding PHI that apply through this BAA to Dell. If Dell uses its affiliates to provide any of the Services, Dell is not required to obtain written assurances from such affiliates or its employees; provided, however, Dell shall be responsible

for any actions of such affiliates and their employees in violation of Dell's obligations under this BAA.

- Information Safeguards: When Dell has possession of PHI, is accessing PHI, or is transmitting Electronic PHI ("ePHI"), it shall (a) use appropriate safeguards as required by the HIPAA Privacy Regulations to prevent the use or disclosure of PHI otherwise than as permitted or required under this BAA; and (b) with respect to ePHI, implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of ePHI as required by, and as more specifically set forth in, the HIPAA Security Regulations. Dell's obligations described above will include additional safeguards required to be taken by Dell pursuant to Section 13401(a) of the HITECH Act. Notwithstanding the foregoing, when Dell is present at a facility of Customer or its affiliates or is accessing or utilizing equipment, software, tools, network components or other information technology owned, leased or licensed by Customer or its affiliates ("Customer Systems"), Dell will comply with Customer's standard safeguards to prevent the use or disclosure of PHI (including Customer's standard administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of ePHI) applicable to such Customer facility or such Customer System, provided Customer has given Dell prior notice of such safeguards in writing or in the same manner as Customer provides notice of such safeguards to its own employees and other contractors. Except as otherwise described herein, Dell is

not responsible for implementing safeguards with respect to the facilities of Customer or its affiliates or Customer Systems. For purposes of clarity, Customer and Dell's respective safeguard obligations are set forth in Table 3 below, "HIPAA Safeguard Responsibility Matrix."

- Security Incidents and Breach of Unsecured PHI: Dell shall report to Customer (a) any use or disclosure of PHI by Dell in violation of its obligations under this BAA of which it becomes aware; and (b) any Security Incident relating to ePHI of which it becomes aware. In addition, Dell shall, following the discovery of a Breach of Unsecured PHI, notify Customer of such Breach in accordance with the HIPAA Breach Notification Rule set forth at 45 C.F.R. § 164.410 Subpart D. With respect to unsuccessful Security Incidents, Dell represents that the significant number of meaningless attempts to access its data, including ePHI, makes it impossible for Dell to report such unsuccessful Security Incidents in real-time or on any regular basis. Accordingly, Customer and Dell agree that this provision constitutes timely notice to Customer of unsuccessful Security Incidents, whether occurring now or in the future, when they do not result in actual unauthorized access, use, disclosure, modification or destruction of ePHI or interference with an information system that contains or processes ePHI, such as but not limited to the following: i) pings on the firewall; ii) attempts to logon to a system, device or database with an invalid password or user name; iii) denial of service attacks; or iv) port scans.
- Compliance Audits: Dell shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Customer's compliance with HIPAA.
- Designated Record Sets: If Dell maintains any Designated Record Sets containing PHI, upon Dell's receipt of a request from Customer for access to PHI about an Individual contained in any Designated Record Set(s) maintained by Dell, Dell shall allow Customer to access such Designated Record Set(s) in the manner originally received by Dell and in the format and on the media in use as of the date of the request in order for Customer to meet its obligations to (a) make the PHI available in accordance with 45 CFR Section 164.524; and (b) amend the PHI in accordance with 45 CFR Section 164.526. As between Customer and Dell, Customer, not Dell, is responsible for responding to requests for access to or amendment of PHI from Individuals pursuant to HIPAA and the HIPAA Privacy Regulations, including, but not limited to, 45 C.F.R. §§164.524, 164.526, and 164.528, as the same may be amended from time to time. If Dell uses or maintains an Electronic Health Record with respect to PHI, in accordance with Section 13405(e) of the HITECH Act, Dell acknowledges that an Individual has a right to obtain from Customer a copy of such information in an electronic format. If the Individual makes an election to obtain from Customer a copy of such information in an electronic format, upon Dell's receipt of written notice from Customer, Dell will as soon as reasonably practicable allow Customer to access any such information in electronic format so that Customer may provide a copy of such information in an electronic format to Customer.
- Accounting of Disclosures: Dell shall document disclosures of PHI it makes and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of such disclosures in accordance with 45 CFR § 164.528; provided, however, with respect to disclosures made at the request of Customer under the Services Description, Customer shall be responsible for recording and tracking any such disclosures required by 45 CFR § 164.528. Upon Dell's receipt of written notice from Customer that Customer has received a request for an accounting of disclosures of PHI regarding an Individual, Dell shall make available to Customer the information collected by it as described above to permit Customer to respond to such request in accordance with 45 CFR § 164.528.
- Minimum Necessary and Limited Data Set: As described in 45 C.F.R. § 164.502(b)(1), when using or disclosing PHI or when requesting PHI from Customer (except for the uses and disclosures described in 45 C.F.R. § 164.502(b)(2)), Dell will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. Dell shall be treated as being in compliance with 45 C.F.R. § 164.502(b)(1) only if Dell limits such PHI, to the extent practicable, to the limited data set (as defined 45 C.F.R. § 164.514(e) (2)) or, if needed by Dell, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively. Dell will determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.
- Marketing Use of PHI: Except as provided in Section 13405(d)(2) of the HITECH Act, Dell will not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless Customer has obtained from the Individual, in accordance with 45 C.F.R. § 164.508,

a valid authorization that includes, in accordance with such section, a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual. Nothing in this Section 9 shall be construed to allow Dell to disclose PHI except as provided in other provisions of this BAA.

- Mitigation: Dell shall mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI by Dell in violation of its obligations set forth in this BAA.
- Consent, Authorization, and Permission: Customer shall obtain and maintain such consents, authorizations and/or permissions, if any, as may be necessary or required under HIPAA, the HITECH Act, or other local, state or federal laws or regulations to permit Customer to disclose PHI to Dell in order for Dell to use and disclose PHI as required or permitted under this BAA. Customer shall promptly inform Dell in writing as soon as Customer becomes aware of any modifications to, restrictions on, defects in, or revocation or other termination of effectiveness of, any such consent, authorization or permission, to the extent any such modifications, restrictions, defects, revocations or terminations affect Dell's permitted or required uses and disclosures of PHI specified in this BAA.
- Limitations in Privacy Practice: Customer shall notify Dell in writing of any limitation(s) in its notice of privacy practices in accordance with 45 CFR § 164.520, to the extent any such limitations affect Dell's permitted or required uses and disclosures of PHI specified in this BAA.
- Uses or Disclosure Restrictions: Customer shall notify Dell in writing of any restriction(s) to the use or disclosure of PHI that Customer has agreed to in accordance with 45 CFR § 164.522, to the extent any such restrictions affect Dell's permitted or required uses and disclosures of PHI specified in this BAA.
- Non-Permitted Use: Without limiting Sections 1(a) – (e), Customer agrees it will not request, and the performance of Dell's obligations under the Services Description will not require, Dell to use or disclose PHI in any manner that would not be permissible if done by Customer.
- Right to Terminate for Breach: If Dell commits a material breach of its obligations in this BAA, Customer may (a) terminate the Services Description (and this BAA) by providing Dell prior written notice if Dell fails to cure such breach within thirty (30) days of its receipt of written notice from Customer specifying the nature of such breach; (b) immediately terminate this Services Description (and this BAA) by providing Dell prior written notice if a cure of such breach is not possible; or (c) report such breach to the Secretary if termination of the Services Description is not feasible.
- Effects of Termination: Upon the termination of this BAA for any reason, Dell shall destroy or return all PHI in its possession by allowing Customer to retrieve any PHI uploaded to the Service, in accordance with the terms of a separate services agreement between Customer and Dell and neither Dell, nor its affiliates or their respective subcontractors shall retain copies of such PHI; provided, however, that if returning or destroying such PHI is infeasible for Dell, Dell shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible for so long as such PHI is maintained by Dell.
- Amendments: The references to the provisions and sections of HIPAA and the HITECH Act in this BAA specifically refer to such provisions and sections as of the Activation Date, and do not include any amendments or changes to such provisions or sections enacted after the Activation Date or any guidance issued by a governmental entity after the Activation Date (including guidance issued pursuant to the HITECH Act). If any final amendments to HIPAA or the HITECH Act are enacted, or any governmental guidance is issued, after the Activation Date, to the extent such amendments or guidance require modifications to the then-current obligations of Customer or Dell under this BAA, Customer and Dell agree to promptly meet and negotiate in good faith to mutually agree on such modifications. Any material modifications to Dell's obligations under this BAA may include changes in financial terms as reasonably required to support such cost of compliance.
- Conflicts: If there is any conflict between the terms of this BAA and the terms of the Service Description respect to the matters covered in this BAA, the terms of this BAA shall control.
- Unless otherwise expressly stated in this Appendix I, where terms conflict, the DIR Contract controls.

HIPAA safeguard responsibility matrix

Standards	Implementation specifications	Customer	Dell
Administrative safeguards			
Security management process	Risk analysis (R)		
	Risk management (R)		
	Sanction policy (R)		
	Information system activity review (R)		
Assigned security responsibility	Assigned security responsibility (R)		
Workforce security	Workforce authorization and/or supervision (A)		
	Workforce clearance procedures (A)		
	Workforce termination procedures (A)		
Information access management	Isolating heath care clearinghouse function (R)	N/A	N/A
	Access authorization (A)		
	Access establishment and modification (A)		
Security awareness and training	Security reminders (A)		
	Protection from malicious software (A) Access establishment and modification		
	Log-in monitoring (A)		
	Password management (A)		
Security incident procedures	Response and reporting (R)		
Contingency plan	Data backup plan (R)		
	Disaster recovery plan (R)		
	Emergency mode operation plan (R)		
	Testing and revision procedure (A)		
	Applications and data criticality analysis (A)		
Evaluation	Security evaluation (R)		
Business associate contracts and other arrangements	Written contract or other arrangements (R)		

Standards	Implementation specifications	Customer	Dell
Physical safeguards			
Facility access controls	Contingency operations (A)		
	Facility security plan (A)		
	Access control and validation procedures (A)		
	Maintenance records (A)		
Workstation use	Workstation use (R)		
Workforce security	Workstation security (R)		
Device and media controls	Media disposal (R)		
	Media re-use (R)		
	Accountability (A)		
	Data backup and storage (A)		

Standards	Implementation specifications	Customer	Dell
Technical safeguards			
Access control	Unique user identification (R)		
	Emergency access procedure (R)		
	Automatic logoff (A)		
	Encryption and decryption (A)		
Integrity	Mechanism to authenticate ePHI (A)		
Person or entity authentication	Person or entity authentication (R)		
Transmission security	Integrity controls (A)		
	Encryption (A)		

(R)= Implementation is required.
(A)= Implementation is addressable. The safeguard must be assessed to whether or not it is a reasonable and appropriate safeguard in your environment. If the safeguard is not implemented, then it is required to document the reason why and also implement an equivalent alternative safeguard if reasonable and appropriate.

Appendix F:

Internet service options: Full service committed bandwidth or committed bandwidth each with optional burst Introduction

to full service committed bandwidth and committed bandwidth

Dell Full Service Committed Bandwidth and Committed Bandwidth Internet Services (the "Internet Service") provide Customer with committed Internet bandwidth and, if purchased, burst bandwidth capability, so that Customer can access its Dell Cloud Service. Full Service Committed Bandwidth Internet Service also includes load balancing features and monthly reporting.

Offer description

Service offer

In order to provide Internet access to your content in your Dell Cloud environment, you will require Internet bandwidth. You should work with your account representative to determine the amount of Internet bandwidth required for your particular use cases.

Service details and options are listed below.

Service details – full service committed bandwidth

Dedicated internet bandwidth

- Provided by the Mbps
- Provided by multiple carriers
- Capped at the dedicated amount that Customer has requested, for example, a 5MB dedicated bandwidth will start to experience performance degradation as the throughput exceeds the threshold that has been set
- Billed on a monthly basis at the rate procured
- Adjustable to accommodate peak load times in the week, month or year

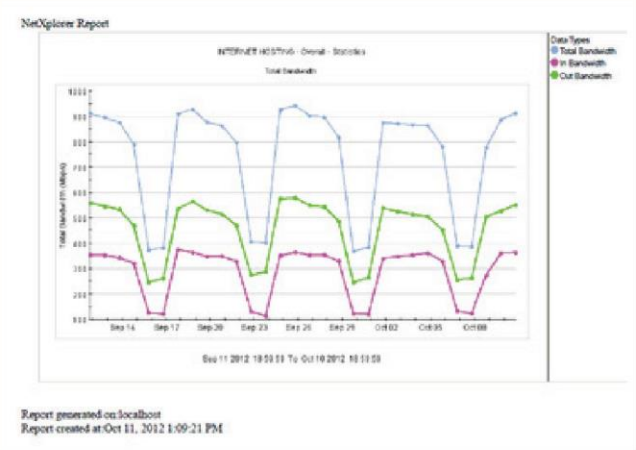
Load balancing

- Available for incoming traffic from the Internet
- Allows for load balancing across virtual servers in Customer's Dell Cloud environment
- A leveraged managed service

- Requests for Move/Add/Change/Deletes (MACDs) are submitted via the service desk for the Dell Cloud service

Reporting

- Bandwidth-related reporting is sent to the Customer-provide email address that has been assigned to the account
- Report frequency is determined by Customer as reports are generated automatically and sent to Customer via email
- Quality of Service (QOS) is not available as Dell cannot control the availability or prioritization across the Internet



Sample report

Service details – committed bandwidth

Dedicated internet bandwidth

- Committed Bandwidth only is available for a lower rate as it excludes reporting and load balancing capabilities
- Provided by the Mbps
- Provided by multiple carriers
- Capped at the dedicated amount that Customer has requested, for example, a 5MB dedicated bandwidth will start to experience performance degradation as the throughput exceeds the threshold that has been set
- Billed on a monthly basis at the rate procured
- Adjustable to accommodate peak load times in the week, month or year

Service details – optional burst

Optional burst provides burst bandwidth capability

- This is NOT a metered service. The burst bandwidth is purchased at a static rate, for example, 5Mbps burst.
- Optional Burst bandwidth is not dedicated; rather burst bandwidth includes shared traffic. Accordingly, performance degradation may occur when Customer is utilizing Optional Burst bandwidth.

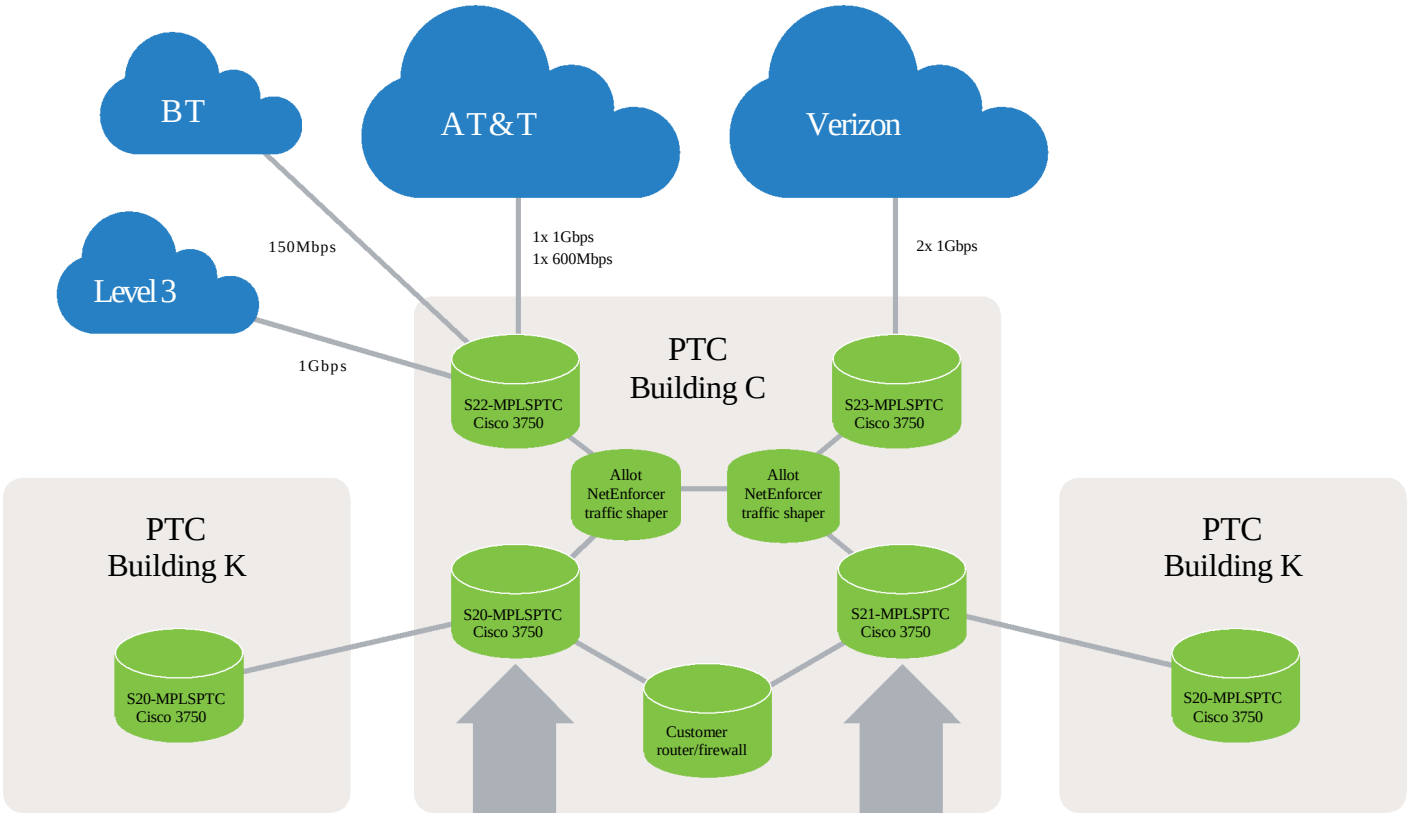
Appendix G:

Leveraged MPLS

Introduction to Leveraged MPLS

Dell Leveraged MPLS (the "MPLS Service") is the MPLS Extranet VPN service provided to support the Service. Dell leverages its MPLS infrastructure so that our Cloud customers can benefit from a high-speed, efficient environment, sophisticated traffic engineering tools and a secure, reliable and redundant data connection to a Dell data center. Ultimately, the MPLS Service will utilize four tier 1 providers (each, a "Carrier"): AT&T, Verizon, Level 3, and BT. Initially, MPLS Service will use AT&T and Verizon. Customers can choose two Carriers to increase end-to-end redundancy and diversity. If Customer chooses two Carriers, in the event the primary link is lost as a result of a network failure, the secondary link will automatically engage resulting in continuous connectivity. Once the primary link is repaired, traffic is then returned to the original path. Dell also supports QOS (quality of service). This is used primarily for voice, video or real-time applications. Dell designs and separates each individual customer's traffic by assigning secure VLANs. The data is shaped according to the quantity of MB each customer requests. This allows for network reporting on utilization. Customer can review the report each month to ensure network optimization and can then increase or decrease the number of MB depending on demand. Customers are responsible for connectivity to the Carrier's cloud.

For illustrative purposes only, the following network diagram shows an example of the leveraged carrier access for the Dell Plano Technology Center (the "PTC"). Please note the Carriers and the bandwidth availability.



Gigabit ethernet RJ45 handoffs
Cloud services
public/private (DCD)

Offer Description

Service offer

Customer will be required to provide the following information as a result of setting up and configuring the MPLS Service:

- Carrier - single/redundant
- Carrier choice - AT&T, Verizon (initially);Level 3, BT (once available)
- Financial ID for internal billing
- Bandwidth – Qty (MB)
- Reporting – Customer e-mail address
- Requestor - email/phone
- Customer Technical Contact - email/phone
- Extranet Agreement (signed by Customer)

Customers must sign an Extranet Agreement with the Carrier and Dell. In order to connect the Customer's private network to Dell's, Dell, collaborating with Customer's network engineer, will update network configurations and enable the networks to effectively pass Customer's data to the Dell Cloud. With the new VLAN assignment and with the passing of information, both engineers will be able to enable the passing of data between Customer and Dell. The last step before connectivity is enabled is a call among the Carrier, Customer's network engineer and Dell. Following the call (and any related follow-on activities that may result therefrom), Customer will be able to transmit data to Dell over the MPLS connection. Customer should work with its account representative to determine the amount of MPLS bandwidth required for Customer's particular use cases.

Service details and options are listed below.

Service details – leveraged MPLS	
Leveraged MPLS access • Provided by the MB • Capped at the committed amount that Customer has requested • Billed on a monthly basis at the rate procured • Adjustable on-demand to accommodate peak load times in the week, month or year	Included
Reporting Dell provides monthly reporting which permits Customer to evaluate the performance and usage of their prescribed network bandwidth.	Included

Appendix H:

Windows Server Instance Support Services

Introduction to Windows Server Instance Support Services

The Windows Server Instance Support Service provides Dell Customers the ongoing administration and engineering support of Windows Servers. Windows Servers are defined as servers that have the Microsoft Windows Operating System running on an Intel processor (or compatible) based hardware platform. The Windows Server Support Service is defined, priced and consumed in per Server Instance units. A Server Instance unit is equal to one Microsoft Windows Operating System instance (OS instance) that is installed on either a physical or virtual server platform.

The Windows Server Instance Support service classifies servers into one of four service options:

		Service Level 1	Service Level 2	Service Level 3	Service Level 4
Server instance support	System administration & engineering	Basic included	Basic included	Standard included	Advanced included
	Monitoring	Basic included	Mid-level included	Mid-level included	Advanced included
	Reporting	N/A	N/A	Standard included	Advanced required
	Add-on support (AD, Citrix & VMware)	N/A	N/A	Optional	Optional
	Support for clustering	N/A	N/A	N/A	Optional
Optional support (DR, custom reporting)		T&M	T&M	T&M	T&M
Service levels	Incident management (max impact/TTR)	Impact $3/_{3\ day}$	Impact $2/_{8\ hr}$	Impact $1/_{4\ hr}$	Impact $1/_{4\ hr}$
	Request management (tiered request fulfillment)	95%	95%	95%	95%
	Problem management (root cause analysis)	None	Requested impact 2's	Impact 1 + requested 2's	Impact 1 + requested 2's
	Server instance availability	95%	99%	99.6%	99.9%
System requirements	Hardware maintenance	NBD	4 hr. response	4 hr. response	4 hr. response
	Dual NIC & power	None	None	Required	Required

Note to architects:
Be sure to include the "required services" in your selections within the Cost Model when creating a deal proposal.

These classification options are selected individually for each Server Instance and are based on:

- the desired support functions and service levels needed to meet the customer's business requirement for that Server Instance
- the minimum system and hardware requirements that impact availability

The price for this service is established and allocated per Server Instance. There are 4 individual Server Instance support rates available. One rate each for tiers 1-4 plus an additional rate for options 3 &4 that includes add-on support for AD, Citrix, VMware Hosts Server Instances and Clustering.

Rate Information

The rates include the Windows Service and Monitoring cost. Additional rates, fees and SKUs are required for other services such as: Data Backup and Retention Service, Service Management, Security Management Service (AV), or any other non-windows service.

The table in the next section outlines the various support functions, service level agreements, system/hardware requirements and prerequisites for each Server Instance unit and how these compare within the classifications. The summary items included in the table are then defined and explained in more detail throughout the remainder of the document.

Server Instance Classification matrix

The table below succinctly describes the various service levels and included service components. Upon request, or as part of the service onboarding process, detailed descriptions of each service option will be provided.

Service description	Option 1	Option 2	Option 3	Option 4
System administration & engineering functions				
Basic services				
Perform ITIL-based incident, change and request management and maintain Server Instance inventory with configuration information	Included	Included	Included	Included
Provide and coordinate fault isolation and break/fix activities and perform routine configuration, maintenance and troubleshooting	Included	Included	Included	Included
Establish and administer routine security and patch procedures	Included	Included	Included	Included
Install, configure and administer backup and recovery systems	Included	Included	Included	Included
Perform ITIL-based activities for problem management	N/A	Included	Included	Included
Standard services				
Perform expanded configuration, maintenance and troubleshooting activities	N/A	N/A	Included	Included
Ensure audit compliance where applicable	N/A	N/A	Included	Included
Perform Server Instance rebuilds activities	N/A	N/A	Included	Included
Administer, configure and troubleshoot Print Server Instances	N/A	N/A	Included	Included
Advanced services				
Monitor capacity usage and provide performance management	N/A	N/A	N/A	Included

Service description	Option 1	Option 2	Option 3	Option 4
Server Instance monitoring tools				
Level of monitoring tools installed and supported	Basic - Connectivity only	Mid-level - OS metrics only	Mid-level - OS metrics, add-ins	Advanced - OS metrics, add-ins
Alerting and automated incident generation provided for	Basic	Mid-level	System thresholds	Thresholds plus plugins
Agent type	Agentless	Agentless	Agentless	Agent based
Server Instance reports available				
Automated reporting available for per server	N/A	N/A	Standard	Advanced
Add-on Server Instance support				
Administer, configure and troubleshoot MS Active Directory Server Instances				
Administer, configure and troubleshoot VMware Host Server Instances				
Server Instance support for clustering				
Server Instances				
Administer, configure and troubleshoot clustering hardware & software solutions	N/A	N/A	N/A	Optional
	N/A	N/A Optional	Optional	
Optional support functions				
	N/A	N/A Optional	Optional	
Various support activities such as: capacity planning, customer reporting, architecture/design and disaster recovery	T&M	T&M	T&M	T&M
Service level agreements aggregated calculation across the customer's Server Instance install base				
ITIL-based incident management (max impact/TTR)	Impact 3 3 day TTR	Impact 2 8 hr TTR	Impact 1 4 hr TTR	
ITIL-based request management (tiered request fulfillment)	95%	95%	95%	
ITIL-based problem management (root cause analysis)	None	Requested impact 2's	Impact 1 + requested 2's	
Server instance availability	95%	99.0%	99.6%	
				Impact 1 4 hr TTR
				98%
				Impact 1 + requested 2's
				99.9% or 99.99% w/opt clustering

Service description	Option 1	Option 2	Option 3	Option 4
System and hardware requirements				
Hardware warranty or maintenance requirement	NBD	4 hr response	4 hr response	4 hr response
Maintain vendor supported operating system level	Required	Required	Required	Required
Server class hardware	Required	Required	Required	Required
Dual power and dual NIC hardware configuration	None	Required	Required	Required
Hardware and software clustering requirement	None	None	None	Required w/ clustering option
Physical locations supported (all sites must meet minimum manufacture environment specifications)	Documented customer site	Dell DC or approved customer site	Dell DC or approved customer DC	Dell DC or approved customer DC

Delivery model

The Dell approach to managing Server Instances revolves around a tiered delivery model utilizing personnel from various global locations that follow standard processes and procedures. This enables the delivery of services to be mapped accurately to the underlying business requirement. The tiered support structure provides the following benefits:

- Greater utilization of support staff by matching the appropriate skill set to the appropriate task
- Ability to maximize automation and standardization
- Reduced disruptions of service from personnel changes compared to single-tiered support models
- Establishing an architecture function to focus on researching emerging technologies and how technology can meet the business needs

The tiered delivery model is illustrated in the following graphic: