Service Description

Dell Workspace-as-a-Service

Introduction to Your Service

Dell Workspace-as-a-Service or (the “Service”) is a managed service offering intended to provide the customer (“Customer” or “you”) with virtual desktops hosted from Dell data centres. This Service Description and the attached appendices (collectively, the “Service Description”) describe the Service, Billing, Provisioning, and Support of the Service.

The Service leverages your existing Microsoft® Active Directory® for end user accounts, authentication, and desktop management group policy objects. Dell will manage the computer accounts and group policy objects through the use of a dedicated Domain Organizational Unit to which you have delegated administrative capabilities to Dell.

Dell Workspace-as-a-Service Components

The Service is composed of the following standard components:

- **Virtual Desktops:**
  - Persistent virtual desktop – most closely resemble the physical desktop your employees are used to. Employees will always connect to the same virtual desktop each time they log in, and they may install additional applications. Employees’ desktop personalization, local documents and other files are retained when the virtual desktop is restarted. New virtual desktops are created based on the golden image, but are stored separately.
  - Non-Persistent virtual desktop – Employees will not connect to the same virtual desktop each time they log in, and the may not install additional local applications. Their desktop personalization and “My Documents” are retained on a file server and applied when the virtual desktop is started.

- **Storage for 5 Gold Images of the default size of those desktops for the initial order up to 1,000 virtual desktops and each subsequent 1,000 virtual desktops thereafter.**

- **Advanced, efficient remote desktop access protocol – Allows for a rich desktop and media experience.**

- **An Internet-facing security gateway – Allows your users remote connectivity to the virtual desktop environment without connecting through your corporate VPN solution.**

- **Highly available service delivery infrastructure – The service infrastructure is designed using highly available, redundant components to extend the resilience designed into Dell’s ISO 27001-certified data centres.**

- **ITIL-based service management, including request, incident, and change management**

1 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
for the Dell Workspace-as-a-Service service environment.

- Dell deployment, monitoring, and management of the Service infrastructure and software, including continuous monitoring and proactive maintenance.
- In addition to the standard features of the Service, there are a number of optional services that may be added to provide the optimum virtual desktop experience. Please contact your Dell sales representative for more information.

The tables below provide a high-level description of the Service features:

### Provisioning

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell Workspace-as-a-Service Network Setup</td>
<td>Provisioning of MPLS circuit and/or establishing VPN connection between Dell data centre and your corporate network</td>
</tr>
<tr>
<td>Dell Workspace-as-a-Service Customer Setup</td>
<td>Creation of Customer Workspace-as-a-Service environment in Dell datacentre</td>
</tr>
<tr>
<td>Ongoing Desktop Provisioning</td>
<td>Dell provisions additional desktops upon request</td>
</tr>
</tbody>
</table>

### Desktop Models

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Persistent Desktop</td>
<td>1 CPU, 2 GB Memory, 25 GB storage.</td>
</tr>
<tr>
<td>Enhanced Persistent Desktop</td>
<td>2 CPU, 3 GB Memory, 30 GB storage.</td>
</tr>
<tr>
<td>Professional Persistent Desktop</td>
<td>2 CPU, 4 GB Memory, 30 GB storage.</td>
</tr>
<tr>
<td>Premium Persistent Desktop</td>
<td>4 CPU, 8 GB Memory, 35 GB storage</td>
</tr>
<tr>
<td>Standard Non-Persistent Desktop</td>
<td>1 CPU, 2 GB Memory, 25 GB storage</td>
</tr>
<tr>
<td>Standby Desktop</td>
<td>Inactive virtual desktop. Ideal for reserving virtual desktop capacity for rapid future deployments or high availability.</td>
</tr>
</tbody>
</table>

### Standard Connectivity

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet access to Virtual Desktops</td>
<td>Allows access to virtual desktops from remote locations without connecting through your corporate network.</td>
</tr>
</tbody>
</table>

### Optional File Server Models

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pilot File Server (Available only for Pilot)</td>
<td>2 CPU, 4 GB Memory, 100GB storage. Primarily for storage of roaming profiles and folder redirection. May also be used for other server applications used to support your virtual desktop environment, such as Microsoft Active Directory, Microsoft Key Management Server, or Dell Wyse® Device Manager.</td>
</tr>
<tr>
<td>Premium File Server</td>
<td>4 CPU, 8 GB Memory, 100GB storage. Primarily for storage of roaming profiles and folder redirection. May also be used for other server applications used to support your virtual desktop environment, such as Microsoft Active Directory, Microsoft Key Management Server, or Wyse Device Manager.</td>
</tr>
</tbody>
</table>
### Optional Desktop/Server Upgrades

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10GB Desktop Storage Upgrade</td>
<td>Increase desktop storage by 10GB</td>
</tr>
<tr>
<td>100GB Server Storage Upgrade</td>
<td>Increase server storage by 100GB</td>
</tr>
</tbody>
</table>

### Configurable Connectivity Methods

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Bandwidth</td>
<td>Bandwidth for Internet access to virtual desktop environment allows users to</td>
</tr>
<tr>
<td></td>
<td>connect to a desktop without first traversing your corporate network.</td>
</tr>
<tr>
<td></td>
<td>Additionally, allows Internet egress from virtual desktops directly from Dell</td>
</tr>
<tr>
<td></td>
<td>Data Centre without additional traffic and latency associated with routing</td>
</tr>
<tr>
<td></td>
<td>your Internet traffic back through your corporate network.</td>
</tr>
<tr>
<td>VPN Connection</td>
<td>Creates VPN connection from Dell data centre to your corporate network.</td>
</tr>
<tr>
<td>MPLS</td>
<td>Establish an MPLS connection between the virtual desktop environment and</td>
</tr>
<tr>
<td></td>
<td>your corporate network for corporate access to virtual desktops and access</td>
</tr>
<tr>
<td></td>
<td>to corporate applications and data from your virtual desktops.</td>
</tr>
</tbody>
</table>

### Optional Connectivity Upgrades

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Balancers</td>
<td>Spread virtual desktops across multiple hosts based on the number of existing</td>
</tr>
<tr>
<td></td>
<td>connections to each host. Load balancers also enhance resiliency by not</td>
</tr>
<tr>
<td></td>
<td>attempting to assign new connections to hosts that are not available.</td>
</tr>
<tr>
<td>Rack Space and Network</td>
<td>Allows you to put additional network or security equipment in the Dell data</td>
</tr>
<tr>
<td>Connection</td>
<td>centre to further manage or protect your virtual desktop environment.</td>
</tr>
</tbody>
</table>

### Optional Desktop and Image Management Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image development and maintenance</td>
<td>Dell will develop an image based on your requirements. Includes quarterly</td>
</tr>
<tr>
<td></td>
<td>application of critical operating system patches.</td>
</tr>
<tr>
<td>Managed Antivirus</td>
<td>VDI optimized antivirus solution managed and monitored by Dell SecureWorks’</td>
</tr>
<tr>
<td></td>
<td>Security Operations Centre.</td>
</tr>
</tbody>
</table>

### Additional Services

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Consulting Service – 4 Hours</td>
<td>Remote consulting to assist customers with Dell Workspace-as-a-Service</td>
</tr>
</tbody>
</table>

### Billing

Provisioning and one-time costs for Optional Add-On Services will be invoiced at the time of ordering. The remaining Service features are available in the following contracts:

- **Monthly Billing Annual Contract:** Once the contract has been executed, the customer is invoiced monthly, in advance. Partial months will be invoiced on a prorated basis. The contract automatically renews for the next year unless automatic renewal is declined in writing at least thirty (30) days prior to the expiration of the term or unless automatic renewal is explicitly disclaimed in the Order Form.

  For example, an agreement is executed on the 15th of the month. The customer will be invoiced for the one-time charges associated with provisioning the Service and any optional Add-On Services, the pro-rated recurring monthly charges from the 15th through the end of the current month.

  The next invoice will be for the monthly recurring charges for the first full month.

3 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
of the Service, which will continue through the term of the Service.

- Paid in Full Annual Contract: Once the contract has been executed, the customer is invoiced for the one-time costs associated with provisioning the Service and any optional Add-On Services as well as twelve (12) months of the recurring monthly fee. The contract automatically renews for the next year unless automatic renewal is declined in writing at least thirty (30) days prior to the expiration of the term or unless automatic renewal is explicitly disclaimed in an Order Form. Customer will receive a prorated refund for the unused portion of the annual contract in the event of an approved contract change request.

- Pilot Contract: Customer is invoiced on contract execution the full cost of the pilot or any pilot options. See pilot terms in Appendix A.

The Activation Date of this Service Description is the date on which the related Order Form is executed by the Customer and accepted by Dell. The Service Start Date for Desktop Models and other optional Add-On Services will commence when access to virtual desktops, as requested in the original order, is provided to the Customer, OR 30 calendar days from contract signing, whichever is shorter. Changes to the service by the customer after contract signing and before Service Start Date will not extend this time limit. Dell will extend this time if any delays are caused by Dell to an amount equal to the delay.

Changes to Dell Workspace-as-a-Service Scope of Services
Changes to the scope of Services, within the terms of this Service Description, will change the cost of the services and will be requested via an approved Change Order Form. Refer to Appendix E for the Change Order Form and the process for submission.

Examples of requests considered changes to the scope of Services requiring a change order:

- Changing number of desktop/server subscriptions
- Change to existing Desktop/Server Profiles distribution.
- Bandwidth Upgrades
- Storage Upgrades
- Provisioning new instance of Service in separate data centre
- Other Service identified in table above

Provisioning
Upon receipt of an Order Form, Dell will assign resources to work with you to configure a Dell Workspace-as-a-Service Customer environment for you ("Provisioning"). Dell will undertake the following Provisioning processes:

- Initiate contact with you to gather the necessary information to complete a successful Provisioning
  - The necessary information will include domain, network, designated Customer contact list, domain service account for Dell’s use, and other relevant information

4 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
• Establish secure VPN backhaul connection (if ordered) to provide an encrypted data path to allow Dell access to the Dell Workspace-as-a-Service specific OU in your Microsoft Active Directory, and to protect the Desktop session traffic between Dell infrastructure and your Microsoft Active Directory, DNS, and DHCP
• Create and configure the Service platform
• Create Desktop models that will be available to you in your Active Directory, and assign user management groups, so that you can administer user access to the virtual desktop models groups
• Provide Dell Workspace-as-a-Service Microsoft Windows starter image to help you build your image with your applications
• Create an account for your company in Dell’s incident management system for incident and service request management
• Provide access to manuals and relevant support documentation as well as information on how to obtain support from Dell.

Infrastructure Management
The Service platform resides in a Dell data centre. Dell will provide security in accordance with the Security Statement provided in Appendix B and incorporated herein. Infrastructure management will be provided in accordance with Appendix F.

Dell offers multiple methods to connect the virtual desktop environment to your corporate network, including Internet bandwidth with VPN connectivity or an MPLS connection, which is recommended for more than 500 users.

Support
Support for the Service is available in English by phone (24 hours x 7 days a week x 365). Support is limited to designated Customer contacts (I.T. personnel or help desk contacts) that are on the designated Customer contact list. Dell provides Support for the infrastructure and Dell Workspace-as-a-Service platform located in the data centre. Any personnel calling in with a request must be on the list of authorized personnel provided by the Customer and have authority to make such requests. The customer is limited to 5 support contacts that will have accounts with the Dell Service Management system, and any updates to this list are conducted via Service requests.

Customers will submit Service Requests through Dell’s Service Request Management System for configuration changes within the scope of the existing services contract. Operational Response Targets are provided in Appendix D.

Examples of service requests include:
• Pool creation/deletion/modification
• Image deployment/maintenance
• Changes to IP addresses to VPN

Remote Consulting Service is available in 4 hour block from Dell. This consulting is limited to advice and support to the Dell Workspace-as-a-Service environment and issues supporting the Dell Workspace-as-a-Service environment. A partial list of supported issues: pool management, configuration issues with service, issues with existing images, and issues with

5 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
end point devices. The Remote Consulting Service will not develop new images for use as this service is available as an option. The Remote Consulting Service does not include site visits. Dell will be sole determiner of when the consulting requested is not within the scope of Dell Workspace-as-a-Service Remote Consulting Service.

Images

Dell Workspace-as-a-Service recommends using either the Dell Starter Image provided with your Service or building a new ‘clean’ image for use in the virtual environment. Converting images designed for the physical environment is extremely time-consuming and the results are usually less than optimal. Dell Workspace-as-a-Service (including Remote Consulting Service) will not support efforts to convert a customer’s physical image to the virtual environment nor will support be available for the tools designed to do this conversion. Dell Workspace-as-a-Service will not support any issues that arise as a result of the customers providing a ‘converted’ image to use on the Dell Workspace-as-a-Service environment. Dell has an optional Image Creation service available to help create your new virtual image.

Customer Responsibilities

You will be responsible for the following activities:

- Obtaining all licenses necessary in connection with all software and applications subject to the Service, including Microsoft Windows Desktop operating system, Microsoft Virtual Desktop Access, and desktop application software
- Configuring and administering Active Directory;
- Providing Dell with an Active Directory Organizational Unit and a service account with delegated authority to add and remove computers and administer Group Policy Objects within that Organizational Unit;
- Creating and removing user accounts for Dell support personnel;
- Assigning users to groups of virtual desktops;
- Supporting end users, including, but not limited to client devices (desktops, notebooks, smartphones thin clients, etc.) and images (operating systems, applications and settings);
- Creating and uploading desktop images;
- Installing and maintaining the operating system and applications within the image;
- Validating application compatibility in a virtual environment and monitoring application performance;
- Performing backups of all existing data, software and programs;
- Managing network connectivity and bandwidth from your network to end users and your network to the Internet, including supporting the VPN hardware and software within your corporate network;
- Ensuring that Customer’s authorized support contacts have purchasing authority to order/change Service;
- Cooperating with and following the instructions given by Dell phone analyst; Supporting Provisioning and any Service upgrade activities;
- Complying with, and ensuring compliance by your end users with, the End User Use Restrictions (set forth in Appendix G attached hereto) applicable to your use of Microsoft products in connection with the Service; and,

6 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
• Complying with, and ensuring compliance by your end users with, the Dell Cloud Solutions Agreement.

Dell Responsibilities
• Obtaining all licenses necessary to provide the Service infrastructure, including Microsoft Windows Server, hypervisor, and VDI software licenses;
• Notifying you to create or delete user accounts for Dell support personnel;
• Deploying desktop images provided by you;
• Providing a starter image optimally configured for virtual desktop environments;
• Creating and removing desktops and managing required Group Policy Objects within the customer provided Active Directory Organizational Unit;
• Maintaining Service platform hardware and software that resides in Dell data centre, including connection from Dell to the Internet and the Dell VPN concentrator;
• Performing incident and request management for platform-level support in accordance with Operational Response Targets in Appendix D; and,
• Ensuring compliance with security statement in Appendix B.

Exclusions
Unless backup or disaster recovery services are included in the Statement of Work, Dell is not responsible for performing any backups of data, software, systems and/or programs. These activities remain at all times the sole responsibility of the Customer.

SUBJECT TO THE LIABILITY SECTION OF THE CLOUD SOLUTIONS AGREEMENT, NOTWITHSTANDING ANYTHING CONTAINED HEREIN TO THE CONTRARY, DELLL WILL HAVE NO LIABILITY FOR LOSS OF, CORRUPTION OF, OR DAMAGE TO DATA OR SOFTWARE OR FOR THE RECOVERY OF DATA OR PROGRAMS OR LOSS OF USE OF SYSTEM(S) ARISING OUT OF OR IN CONNECTION WITH THE SERVICE.

The terms of this Service Description do not confer on the Customer any warranties which are in addition to the warranties provided under the terms of the Cloud Solutions Agreement.

Miscellaneous
No hardware is being transferred, sold, leased or licensed to Customer under this Service Description. To the extent Dell uses hardware or software as part of its delivery of the Service, such hardware or software will be licensed, owned or otherwise held by Dell. The Service can be hosted out of data centres in both the United States and the European Economic Area. During discovery, Customer will select which region(s) to host the Service.

Dell may modify the Service (including modifications to the software and other elements of the Dell Infrastructure) at any time, without prior notice, provided the modification does not materially denigrate the functionality of the Service.

7 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
Terms & Conditions
The terms and conditions in the Cloud Solutions Agreement will govern the provision of the Service. The Cloud Solutions Agreement is available at www.Dell.com/cloudterms. By entering into this Service Description, Customer acknowledges Customer has read and understood the Cloud Solutions Agreement and Customer agrees to be bound by the Cloud Solutions Agreement.

Availability of the Service varies by country. To learn more, customers should contact your sales representative for more information.
Appendix A: Pilot

The Dell Workspace-as-a-Service pilot is designed to allow Customers to verify full production operations on a reduced scale for a fixed period of time and then quickly expand into full scale production. There are no differences in the pilot infrastructure and the production infrastructure however; some limitations will exist to reflect the scale and short time period of the pilot.

The pilot length is 60 days from contract signing. This will include approximately 15 days for provisioning and the remainder for pilot environment use. The pilot may be extended in 30-day increments up to 120 day total pilot length (2 extensions).

The pilot will adhere to the terms and conditions of the Dell Workspace-as-a-Service Service Description unless otherwise noted in this appendix.

Pilot Build Out

The Pilot is designed to allow maximum use for the Customer of one host. Therefore the Customer has options in selecting the profiles needed for its particular test cases without impacting the cost of the pilot.

The pilot price includes a one-time setup fee with the first host. This does not include the VPN backhaul circuit which must be purchased separately if needed.

A Pilot File Server is included in all pilot builds.

In order to calculate the maximum seats at the various profiles the following chart should be used.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Standard</th>
<th>Enhanced</th>
<th>Professional</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum if one profile used on host</td>
<td>50</td>
<td>32</td>
<td>25</td>
<td>12</td>
</tr>
<tr>
<td>Profile Factor – multiply by number of seats desired – Total must be less than 50.</td>
<td>1</td>
<td>1.5</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

Example:

A Customer desires the following desktop profile distribution:

Standard – 25, Enhanced – 6, Professional – 4, Premium – 2

Standard = 25 * 1.0 = 25
Enhanced = 6 * 1.5 = 9
Prof = 4 * 2.0 = 8
Premium = 2 * 4.0 = 8

Sum of the above is 50; therefore this profile distribution is valid for the pilot.

If a Customer desires a higher volume pilot the option exists to purchase another host. The total profile ratio must be <=100 for the second host. The total profile ratio for a two-host
pilot must be \(<150\).

**Billing**

See Billing of Service Description.

**Provisioning**

The provisioning process remains unchanged as the infrastructure used for production is the same as used for pilot.

**Exceptions to the Full Production Service Description**

Pilots are intended for the Customer to test use cases, images and applications and Dell response and support. Customers should not use the pilot Dell Workspace-as-a-Service for their production work.

The 99.5% Monthly Service Uptime Percentage applies to the pilot since it is on the production environment; however, no credits will be authorized for submission during the pilot if the Uptime Percentage is not achieved.

All Standard Service Features are included except for the following

- Standby Desktops are not valid for pilot

Optional / Configurable Services not available with the pilot:

- MPLS Network Connectivity (unless MPLS connectivity already established with Dell data centre)
- Additional Rack Space and Network Connection
- Managed Antivirus
Appendix B: Security Statement

Commitment to Security

Dell Workspace-as-a-Service is designed and built to address key security aspects, including:

Integrity: Through Internet Protocol Security (IPsec), Secure Socket Layer (SSL), and secure VPN 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 within their virtual environment. In addition to the confidentiality enabled through secured network connections, your existing domain and desktop security controls are still available and controlled by you.

Availability: The Service uses mission-critical, highly robust, top-tier data centres, designed to enable service availability at all times.

Overview

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

Physical controls, including environmental controls, are designed to protect the physical environment; for example, access controls, fire prevention systems, cooling systems, exit routes, security personnel and datacentre surveillance monitoring.

Technical controls, also called logical controls, are selected and implemented to mitigate risk; for example, firewalls, intrusion detection and prevention systems, and encryption mechanisms.

Administrative controls include policy and procedures; for example, security and escalation policies, log audits, vulnerability scanning and penetration testing.

---

1 The controls outlined in this Appendix are designed to provide strong data security safeguards that meet the needs of a typical user. They are not intended or designed to address all industry specific requirements that are driven by regulatory requirements such as HIPAA. Users with specific data security requirements that exceed the controls listed in this Appendix should discuss alternative cloud solutions with their Dell representative.
Physical Controls

Dell’s Service data centres are designed to support and protect mission-critical operations. These data centres provide multi-level physical security features and a rigidly-controlled operating environment to help protect customer assets and operations. Dell’s Service datacentres are audited annually to maintain ISO/IEC 27001 and other certifications.

Access and Security Controls
Access to Dell’s Service datacentres is highly controlled. All entrances are monitored and have alarms for protection. These datacentres are staffed with 24-hour security officers to augment physical security features, providing protection of your operations.

CCTV Digital Recorders
CCTV security cameras monitor designated sensitive areas.

Fire Suppression
Industry standard fire suppression systems for multi-tenant datacentres are in use.

Environmental Controls
Dell’s Service data centres are constructed to meet the highest standards of redundancy. Service datacentres 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 defences are used to protect customer information and strictly control network access to the Dell datacentre. Customers connect with the Service via MPLS, IPsec VPN, and SSL connections to provide industry-standard link security to help ensure that customer data cannot be 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.

Customer isolation is implemented through Virtual Routing and Forwarding (VRF), as well as Layer 2 VLANs.

VM processing is performed within a single region only. Data hosted on virtual machines that are provisioned in Slough is not replicated or otherwise transferred to Dell datacentres located in other regions. Customer account information, however, is processed in other regions for billing and support. In addition, the Service infrastructure in the Slough datacentre will be monitored from Dell SecureWorks Security Operations Centres (SOC) located in the United States. Dell subscribes to the provisions of Directive 95/46/EC for data privacy and protection.

Firewalls
Customer data transfers are made from the customer’s environment to the Service system via standard MPLS circuits or an IPsec VPN connection through the Customer’s firewall. All non-required firewall ports are blocked on the Dell Workspace-as-a-Service 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 Centre Monitoring
Dell SecureWorks monitors all firewalls, web application firewalls and other network probes within the Service infrastructure to facilitate early detection of any attempted data breaches.

Access Controls
Access to 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 exceptions basis to enable incident response and forensic investigations by recognized experts in this area.

Vulnerability Scanning
Internal and external vulnerability scans are performed on Dell’s cloud infrastructure periodically and after any significant change in the network.

Administrative Controls
Datacentre Access History
Physical access history to the Dell datacentres is recorded.

Personnel Security
All Dell employees with access to the Service environment are responsible for compliance with Dell information security policies and standards. As part of the employment process, 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 Dell’s standard on Acceptable Use is displayed upon login to servers, desktops and notebooks. Dell’s 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 Service infrastructure, systems and applications are managed 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. The procedures include incident analysis, containment, response, remediation, reporting and procedures for returning to normal operations.
Appendix C: Service Level Agreement for Dell Workspace-as-a-Service

During the term of the applicable Order Form between Dell and Customer for the Service, Dell will use commercially reasonable efforts to achieve a Monthly Uptime Percentage of at least 99.5% for the Dell Infrastructure for any calendar month.

Dell will report Monthly Uptime Percentage on a Service wide basis which is inclusive of all production infrastructures and not for individual customer environments. Dell acknowledges that individual customer monthly uptime percentage may be different (higher or lower) due to impact of an event on a smaller portion of the production environment. If Dell does not meet the SLA on Monthly Uptime Percentage with respect to an individual customer’s environment that customer has the ability to request a credit, assuming that customer’s account is current and not suspended.

Definitions
The following definitions apply to this SLA (all times in minutes unless otherwise noted). All definitions are “Service” based.

- **Dell Infrastructure**: The network and hardware infrastructure which extends from the Service computing resources to the data centre-located router that provides the outside interface of each of Dell’s WAN connections to its backbone providers, in addition to the data centre infrastructure which includes the HVAC, managed power systems, backup generators, and battery backup systems, as well as the servers, the storage, and the network related to the Service.

- **Excluded Minutes**: Minutes of downtime that (i) occur prior to Provisioning being completed (as described in the Provisioning section of the Service Description); (ii) result from Service unavailability caused by maintenance of the platform used to provide the Service which does not exceed the pre-determined unavailability window for such maintenance; (iii) result from Service unavailability caused by events outside the reasonable control of Dell or its subcontractors, including failure or unavailability of the Customer’s systems, the Internet, or any other service or third-party used by Customer to use, connect to, or access the Service; and (iv) activities by Customer resulting in the inability to use the Service. Excluded Minutes are not counted toward Monthly Calendar Minutes.

- **Monthly Calendar Minutes**: The total number of minutes in a given calendar month minus any Excluded Minutes.

- **Monthly Uptime Percentage**: Percentage of time the Service is available in a given calendar month taking into account exclusions and outages. See SLA Calculation set forth below.

- **Monthly Service Downtime**: Total number of minutes per service outage (excluding Excluded Minutes) multiplied by the total number of Service Subscriptions rendered unusable or inaccessible by the incident in a calendar month.

- **Monthly Service Minutes**: Monthly Calendar Minutes multiplied by the total number of Service Subscriptions.

- **Service Subscription**: The total number of virtual desktop subscriptions (includes file servers) for all customers inclusive.
SLA Calculation:

**Service Based** (Reported monthly & calculated by Dell Workspace-as-a-Service):

Monthly Uptime Percentage = \( \frac{100 \times (\text{Monthly Service Minutes} - \text{Monthly Service Downtime})}{\text{Monthly Service Minutes}} \)

**Credits**

If Dell does not meet this SLA during the term, and so long as your account with Dell is current and not suspended, you may be eligible to receive the below-referenced Credits.

If Dell does not meet the SLA for a particular calendar month during the term set forth in the Order Form, Dell will, at Customer’s request, provide the applicable credit (“Credit”) set out below with respect to charges billed for the Service in the month of occurrence:

<table>
<thead>
<tr>
<th>Monthly Uptime Percentage</th>
<th>Credit Percentage Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>100% - 99.5%</td>
<td>0% of charges billed for the Service in month of occurrence</td>
</tr>
<tr>
<td>99.49% - 99.11%</td>
<td>10% of charges billed for the Service in month of occurrence</td>
</tr>
<tr>
<td>&lt;= 99%</td>
<td>15% of charges billed for the Service in month of occurrence</td>
</tr>
</tbody>
</table>

Fractions of a minute will be rounded-up to the next highest minute.

**Example:** Assume 30 days in a calendar month. Assume a 500 seat customer with outage from power failure for 3 servers that results in 250 seats being inaccessible for 440 minutes. Also assume during the month a planned service wide maintenance event with duration of 25 minutes impacted all 500 seats. Assume no other customers.

Excluded Minutes = 25

Monthly Calendar Minutes = 43,200 – 25 = 43,175

Service Subscriptions = 500

Monthly Service Minutes = 43,175 x 500 = 21,587,500

Monthly Service Downtime = 440 x 250 = 110,000

Uptime percentage = \( \frac{100 \times (\text{Monthly Service Availability} - \text{Monthly Service Downtime})}{\text{Monthly Service Availability}} \)

Therefore:

Monthly Uptime Percentage = \( \frac{100 \times (21,587,500 \text{ min} - 110,000 \text{ min})}{21,587,500 \text{ min}} \) = **99.49% for a credit of 10%**

**Incidents**

Incidents are submitted through Dell’s incident management system.
Maximum Credit
The maximum Credit available to Customer if Dell is unable to meet the SLA is up to 15% of the monthly fees for the calendar month of the occurrence. Any “credit” that Dell may owe you, such as a Credit for a failure to meet the SLA, will be applied to fees due from you for the Service, and will not be paid to you as a refund. All claims for Credit are subject to review and verification by Dell, and all Credits will be based on Dell’s measurement of its performance of the Service and will be final.

Example: As noted above, if there is an SLA breach–which results in a 10% Credit toward the amount due for the month of occurrence. If Customer’s monthly fees for Service equal $25,000 during the month of the occurrence then Customer will receive a credit for $2500 on the next invoice. In this case, the maximum Credit allowed would be up to $3750 during the month of the occurrence.

Customer’s sole remedy, and Dell’s sole liability, with respect to Dell’s inability to meet any SLA is the Credits described above and Customer explicitly disclaims any and all other remedies, whether in law or equity.

Claim Procedure
To receive a Credit, a Customer is responsible for making a claim alleging Dell’s failure to achieve the SLA within 30 days of the last date of the reported Downtime. The Claim must include the incident ticket numbers reporting the failure. The claim must be sent by e-mail to the following address: Dell_Cloud_SLA_Claims@Dell.com. The e-mail must include the following information in a form provided by Dell Workspace-as-a-Service on request:

- Customer name
- Customer account number, if applicable
- Name of the Service to which the claim relates, (e.g. Dell Workspace-as-a-Service)
- Customer contact name
- Customer contact e-mail address
- Customer contact telephone number
- Date(s) and time(s) for each claim for downtime
- Incident ticket number
- Number of end users affected per incident
- Additional details, if needed.
- Calculation of Customer Uptime percentage experienced (see attached)
Appendix D: Operational Response Targets

Although Dell strives to achieve the below-listed operational response targets with respect to Incident Response Times and Service Requests, failure to achieve these targets will not give rise to any liability.

“Incident Response Times” is defined as the elapsed time between submission of an incident to Dell and the acceptance by a technician of an assignment to address the incident.

“Service Requests” are defined as changes within the scope of the existing Workspace-as-a-Service order which do not incur additional charges; for example, pool creation, deletion, and modification or deploying your new images. Dell target completion of these services at 5 business days.

“Severity Level 1” is defined as a problem where the majority of End Users who use the Service are severely affected which severely affects the Customer’s ability to conduct its business operations, and there is no workaround for the applicable problem.

“Severity Level 2” is defined as a problem where the majority of End Users who use the Service are affected which moderately affects the Customer’s ability to conduct its business operations because performance is degraded or functionality of the affected item is limited.

“Severity Level 3” is defined as a problem where a reasonably limited number of End Users who use the Service are affected and the effect on Customer’s ability to conduct its business is limited.

“Severity Level 4” is defined as a problem where a single End User is affected and the effect on Customer’s ability to conduct its business operations is limited.

### Operational Response Targets

<table>
<thead>
<tr>
<th>Incident Response Times</th>
<th>Service Requests</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity Level 1 – 98% with 60 minutes</td>
<td>5 business days</td>
</tr>
<tr>
<td>Severity Level 2 – 98% within 60 minutes</td>
<td></td>
</tr>
<tr>
<td>Severity Level 3 – 98% within 8 business hours</td>
<td></td>
</tr>
<tr>
<td>Severity Level 4 – 98% within 16 business hours</td>
<td></td>
</tr>
</tbody>
</table>

Service Requests times are operational targets and are expected to support the normal operations of the Dell Workspace-as-a-Service service for all of our customers. A customer planning a large number of requests to support a significant change in business or use case should contact Dell Workspace-as-a-Service Delivery in advance to prevent any delays caused by an excessive number of requests.
Appendix E: Changes to Existing Contract

Any change to the service that will impact the scope of the Service must be submitted via the Change Order Process outlined below.

Change orders submitted for an existing order that has not been implemented and assigned a Service Start Date will not impact delivery dates for the original order.

Examples of requests considered changes to the scope of Service requiring a change order:

- The addition of virtual desktops above the contracted amount
- Network bandwidth upgrades
- Desktop or file server storage upgrades
- Provisioning new instance of service in separate data centre

Change Order Process

Customer determining need for additional services will contact the Dell Workspace-as-a-Service Delivery Manager via the Service Desk. The Dell Workspace-as-a-Service Delivery Manager will create an order based on your request and submit to you for approval. Customer will return the approved order to the Dell Workspace-as-a-Service Delivery Manager who will process the order and submit necessary work orders to deliver requested services.

Note: Normal additions (i.e., 100-200 desktops) to service will be implemented within the delivery targets in this Service Description. Significant additions to service should be communicated to your Dell Workspace-as-a-Service Delivery Manager as early as possible for planning purposes and to establish delivery expectations.

Billing

The Activation and Service Start dates for this order are consistent with the original order terms.

The impact to your billing will be determined by the original contract type. Invoicing will remain as it is in your original contract for services. Partial months incurred by the submission of the Change Order and the Service Start Date will be invoiced on a prorated basis.

Unless otherwise defined on the Change Order, the end date of the Change Order will co-terminate with the end date of your base contract. For example, if you add 500 desktops in month 6 of a 12 month contract, the Change Order will terminate in 6 months.
Appendix F: Maintenance Practices

Maintenance conducted on the Service infrastructure falls under different categories (listed below) based on impact to Customer and to the Service.

Non-Customer Impact
Maintenance that has no risk of impact to Customer’s Service availability. For example, adding additional hardware for normal Customer expansion.

Moderate Customer Impact
Maintenance that impacts Customer’s Service availability for less than two hours.

Significant Customer Impact
Maintenance (i) to correct significant Service availability issue, (ii) maintenance that impacts Customer’s Service availability for more than 2 hours, or (iii) that requires Customer to perform modification to processes, practices and/or infrastructure.

Maintenance scheduling will be performed as follows:

Planned Maintenance
Normally performed during pre-established maintenance windows or as a scheduled event (for example, system wide upgrades).

Unscheduled/Urgent Maintenance
Performed as necessary to respond to an event that is or may cause a disruption in Service or an impact to the Service reliability.

Communication
Communication procedures are established by Dell so that proper information is distributed regarding the status of the Service environment and to coordinate any actions.

Customer will provide 2 names during onboarding that will be contacted on all required maintenance events. The communications of these events within the Customer’s organization are the Customer’s responsibility.

Communication timeframes, which are aspirational only, are set forth below:

<table>
<thead>
<tr>
<th>Impact</th>
<th>Planned Maintenance</th>
<th>Unplanned/Urgent Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Customer Impact</td>
<td>No Notice</td>
<td>No Notice</td>
</tr>
<tr>
<td>Moderate Customer Impact</td>
<td>2 weeks (10 business days)</td>
<td>ASAP not to exceed 1 hours</td>
</tr>
<tr>
<td>Significant Customer Impact</td>
<td>30 days</td>
<td>ASAP not to exceed 1 hours</td>
</tr>
</tbody>
</table>

19 Service Description: Dell Workspace-as-a-Service

Version 1.0 January 2014
Planned Maintenance

Dell routinely conducts maintenance on the infrastructure platform our customers utilize. This may include (but is not limited to) expansion of or modification to hardware, software, storage and network components.

Dell will normally adhere to the following maintenance windows for all countries where Dell Workspace-as-a-Service is offered.

Service Maintenance Windows

US
Tuesday and Thursday 7:00 PM to 7:00 AM CST for maintenance that is not expected to require more than 2 hours of potential service interruption.

Sunday 12:00 AM to 6:00 PM CST for maintenance with a potential service interruption of more than 2 hours.

EMEA
Tuesday and Thursday 7:00 PM to 7:00 AM GMT for maintenance that is not expected to require more than 2 hours of potential service interruption.

Sunday 12:00 AM to 6:00 PM GMT for maintenance with a potential service interruption of more than 2 hours.

Significant Planned Event

Periodically there may be a significant planned maintenance event (for example, platform software version change) that will involve an interruption in the Service and/or require actions to be taken by a significant portion of our customers. Such actions typically include upgrading the Service agent on the desktop image(s). These events are normally scheduled for weekend or holiday periods when usage of the Service is lowest. Dell will normally communicate the schedule and scope of these events at least 30 calendar days in advance in order to facilitate Customer planning and support. These events will usually need close communications between Dell and the Customer. Dell will set up any required bridge lines and communicate connection information.

Unscheduled Maintenance

In the event an issue occurs that results in a disruption of Service or an imminent disruption of Service that cannot, in Dell’s reasonable assessment, be scheduled at the next maintenance window, Dell will perform the necessary actions to place the Service in the most stable condition and conduct maintenance to bring Service back to full capability. If full capability cannot be achieved, Dell will place Service in the highest functional capability possible until permanent repairs can be made.

The event occurring will be communicated to the Customers as soon as conditions allow.

A bridge line will normally be established by Dell in the event of a significant system outage to communicate event status and coordinate any actions with the Customer.

Maintenance necessary to restore service will not require customer approval to implement.
Customer-Initiated Maintenance

On occasion, Customer may want to make changes to its environment that could impact the Service and that may require action by Dell to ensure continued Service (for example, Customer/Provider Firewall rule changes, Customer/Provider VPN settings, DHCP Server changes).

Changes to the initial Service configuration may require Dell to follow internal change control and notification processes if such changes are to be supported. Any proposed change will be communicated to Dell via a Service support request a minimum of 2 weeks (10 business days) prior to the date the scheduled change is to begin.

In the event of a Service-impacting unplanned event on the Customer infrastructure requiring Dell to perform modifications to Service configuration, the Customer will call in an incident and Dell will respond per the incident response targets in Appendix D.

Dell cannot guarantee that all requested modifications from Customer will be implemented.
Appendix G:
End User Restrictions

Customer (i) will prohibit its end users from removing, modifying or obscuring any copyright, trademark or other proprietary rights notices that are contained in or on the Microsoft products (the “Products”); (ii) will prohibit its end users from reverse engineering, decompiling or disassembling the Products, except to the extent that such activity is expressly permitted by applicable law; (iii) disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages, whether direct, indirect, or consequential, arising from the Service; and (iv) permits Dell to make disclosures required by Dell under Dell’s Services Provider License Agreement with Microsoft.