NTT DATA Service Description

NTT DATA Workspace-as-a-Service

1. Introduction to Your Service

1.1. NTT DATA Workspace-as-a-Service (the "Service") is a managed service offering intended to provide the customer ("Customer" or "you") with virtual desktops and/or applications hosted from NTT DATA data centers. This Service Description and the attached appendices (collectively, the "Service Description") describe the Service, billing, provisioning, and support of the Service. Your quote, order form or other mutually-agreed upon form of invoice or order acknowledgment (as applicable, the "Order Form") will include the name of the service(s) and available service options that you purchased. For additional assistance or to request a copy of your service contract(s), contact NTT DATA Technical Support or your sales representative.

1.2. The Service leverages your existing Microsoft® Active Directory® for end user accounts, authentication, and desktop management group policy objects. NTT DATA 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 NTT DATA.

2. NTT DATA Workspace-as-a-Service components

The Service is composed of one or more of the following selected virtual desktops or Application Delivery Hosts and related service elements

2.1. Virtual Desktops:

2.1.1. Non-persistent virtual desktop –End users will connect to a standard desktop with the Customer determined Gold Image each time they log in. Users' desktop personalization and "My Documents" are retained on a file server and applied when the virtual desktop is started. End users will not have administration rights and cannot install additional applications.

2.1.2. Persistent virtual desktop – most closely resembles 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.

2.1.3. Storage for 5 Gold Images, of the default size of those desktops, i.e. per order of up to 1,000 virtual desktops and/or each subsequent 1,000 virtual desktops thereafter.

2.1.4. Table 1 below provides a high-level description of the Virtual Desktop Service features:

Desktop models	
Service	Description
Standard Desktop	1 vCPU, 2 GB Memory, 30 GB storage.
Enhanced Desktop	2 vCPU, 3 GB Memory, 30 GB storage.
Professional Desktop	2 vCPU, 4 GB Memory, 60 GB storage.
Premium Desktop	4 vCPU, 8GB Memory, 120 GB storage.
Standby Desktop	Inactive virtual desktop. Ideal for reserving virtual desktop capacity for rapid future deployments or high availability.

2.2. Application Delivery Hosts for Shared Session Desktops or Published Applications:

2.2.1. An Application Delivery Host is comprised of one or more Shared Session Desktops or Published Applications and associated Gold Image.

2.2.2. Shared Session Desktops provide workers with a virtual desktop enabling them to work with applications and files within the Application Delivery Host.

2.2.3. Published Applications allow workers to connect to a defined set of virtual applications without the need for a full virtual desktop.

2.2.4. Storage for 5 Gold Images with a maximum of 300GB in total storage for each set of 5 Application Delivery Hosts. Purchased as individual Application Delivery Hosts, image storage will be collectively allocated in groups of 5 hosts.

2.2.5. Publication of up to 5 applications per Gold Image.

2.2.6. Table 2 below provides a high-level description of the Application Delivery Host Service features:

Application Delivery Host	
Application Delivery Host	Minimum of 2 CPU, 256 GB Memory, 500 GB storage.

2.3. Common Service Elements:

2.3.1. Advanced, efficient remote desktop access protocols – Allows for a rich desktop and media experience.

2.3.2. An internet-facing security gateway – Allows your users remote connectivity to the virtual desktop environment without connecting through your corporate virtual private network (VPN) solution.

2.3.3. Highly available service delivery infrastructure – The service infrastructure is designed using highly available, redundant components to extend the resilience designed into NTT DATA's ISO 27001-certified data centers.

2.3.4. ITIL-based service management, including request, incident, and change management for the NTT DATA Workspace-as-a-Service service environment.

2.3.5. NTT DATA deployment, monitoring, and management of the Service infrastructure and software, including continuous monitoring and proactive maintenance.

2.3.6. NTT DATA can provide assistance in determining the best methods and technologies for your enterprise to manage internet access for virtual desktop and application users. Consult with your NTT DATA sales representative to discuss your requirements.

2.3.7. In addition to the standard features of the Service, there are a number of optional services that may be added to provide the optimum user experience. Please contact your NTT DATA sales representative for more information.

2.3.8. Table 3 below provides a high-level description of common Service features, including the optional add on service features:

Provisioning	
Service	Description
NTT DATA Network Setup	Provisioning of multiprotocol label switching (MPLS) circuit and/or establishing VPN connection between NTT DATA data center and your corporate network.
NTT DATA Customer Setup	Creation of Customer environment in NTT DATA datacenter.
Ongoing Service Provisioning	NTT DATA provisions additional desktops or application delivery components (Hosts & VM's), upon request.
Standard connectivity	
Service	Description
Internet access to NTT DATA Workspace environment	Allows access to NTT DATA Workspace environment from remote locations without connecting through your corporate network.
Configurable connectivity methods	
Service	Description
Internet Bandwidth	Bandwidth for: • Access to NTT DATA Workspace-as-a-Service environment over point to point VPN from the corporate network. • Access to NTT DATA Workspace-as-a-Service environment for remote users directly from the internet over an SSL secure gateway, • Internet egress from virtual desktops directly from NTT DATA Data Center without additional traffic and latency associated with routing your internet traffic back through your corporate network.
VPN Connection	Creates VPN connection from NTT DATA data center to your corporate network.
MPLS	Establish an MPLS connection between the NTT DATA Workspace environment and your corporate network for access to corporate applications and data to and from your NTT DATA Workspace environment. An MPLS connection is recommended for more than 500 users.

2.4. Optional Service Elements:

2.4.1. In addition to the standard features of the Service, there are a number of optional services that may be added to provide the optimum user experience. Please contact your NTT DATA sales representative for more information.

2.4.2. Table 4 below provides a high-level description of optional Service features:

Optional file server models	
Service	Description
Pilot File Server (Available only for Pilot)	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 NTT DATA Workspace environment, such as Microsoft Active Directory, Microsoft Key Management Server, or NTT DATA Wyse® Device Manager.
Premium File Server	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 NTT DATA Workspace environment, such as Microsoft Active Directory, Microsoft Key Management Server, or NTT DATA Wyse Device Manager.
Optional storage upgrades	
Service	Description
10GB Storage Upgrade	Increase storage by 10GB.
100GB Storage Upgrade	Increase storage by 100GB.
Optional connectivity upgrades	
Service	Description
Rack Space and Network Connection	Allows you to put additional network or security equipment in the NTT DATA data center to further manage or protect your NTT DATA Workspace environment
Optional image management services	
Service	Description
Image development and maintenance	NTT DATA will develop an image based on your requirements. Includes quarterly application of critical operating system patches.
Managed Antivirus	VDI optimized antivirus solution managed and monitored by NTT DATA SecureWorks' Security Operations Center.
Additional services	
Service	Description
Remote Consulting Service – 4 Hours	Remote consulting to assist customers with NTT DATA Workspace configuration.

3. Billing

3.1. Provisioning costs and one-time costs for Optional Services will be invoiced at the time of ordering.

3.2. Recurring Service features are available in the following options:

3.2.1. Monthly Billing Annual option: Effective the Activation Date, the Customer is invoiced monthly, in advance. The provisioning costs and add-on costs will be invoiced at the time of ordering Partial months will be invoiced on a prorated basis. The Service 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 of the Service, which will continue through the term of the Service.

3.2.2. Paid in Full Annual option: 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 Service 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.

3.2.3. Pilot option: Customer is invoiced on Activation Date the full cost of the pilot or any pilot options. Specific terms for the pilot option are provided in Appendix A.

3.3. The activation date ("Activation Date") of the Services provided under this Service Description is the date on which the related Order Form is executed by the Customer and NTT DATA. The Service Start Date for Desktop Models, Application Delivery Hosts, and other optional Add-On Services will commence when access to your NTT DATA Workspace environment, as requested in the order form, is provided to you OR thirty (30) calendar days from Activation Date , whichever is shorter (the "Service Start Date"). Changes to the service by the Customer after contract execution and before Service Start Date will not extend the Service Start Date. NTT DATA will extend the Service Start Date if any delays are caused by NTT DATA to an amount equal to the delay.

4. Changes to scope of services

4.1. 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/application delivery host/server subscriptions
- Change to existing Desktop/Server Profiles distribution
- Bandwidth Upgrades
- Storage Upgrades
- Provisioning new instance of Service in separate data center
- Other Service identified in table above

5. Provisioning

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

5.1.1. 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 NTT DATA's use, and other relevant information.

5.1.2. Establish secure VPN backhaul connection (if ordered) to provide an encrypted data path to allow NTT DATA access to the NTT DATA Workspace-as-a-Service-specific organizational unit (OU) in your Microsoft Active Directory, and to protect session traffic between NTT DATA infrastructure and your Microsoft Active Directory, domain name service (DNS), and dynamic host configuration protocol (DHCP).

5.1.3. Create Desktop and/or server 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 and/or server models groups.

5.1.4. Create and configure the Service platform.

5.1.5. Provide NTT DATA Workspace-as-a-Service Microsoft Windows or Windows Server Starter Image(s) to help you build your image with your applications.

5.1.6. Create an account for your company in NTT DATA's incident management system for incident and service request management.

5.1.7. Provide access to manuals and relevant support documentation as well as information on how to obtain support from NTT DATA.

6. Infrastructure management

6.1. The Service platform resides in a NTT DATA data center. NTT DATA 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.

6.2. NTT DATA offers multiple methods to connect the NTT DATA Workspace environment to your corporate network, including internet bandwidth with VPN connectivity or an MPLS connection, which is recommended for more than 500 users.

7. Support

7.1. 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. NTT DATA provides Support for the infrastructure and NTT DATA Workspace-as-a-Service platform located in the data center. The Customer is

limited to 5 designated support contacts that will have accounts with the NTT DATA Service Management system, and any updates to this list are conducted via Service requests.

7.2. Customers will submit service requests ("Service Requests") through NTT DATA's Service Request Management System (NTT DATA SRMS) for configuration changes within the scope of the existing services contract. Operational Response Targets are as provided in Appendix D.

Examples of Service Requests include:

- Desktop pool creation/deletion/modification
- Image deployment/maintenance
- Changes to internet protocol (IP) addresses to VPN

7.3. Remote consulting service ("RCS") is available in four (4) hour block from NTT DATA. You may purchase the necessary amount of RCS time block in consultation with NTT DATA and ordering them. The RCS shall become available to you upon execution of an Order for these services. This RCS is limited to advice and support to the NTT DATA Workspace-as-a-Service environment and issues supporting the NTT DATA Workspace-as-a-Service environment, for example pool management, configuration issues with service, issues with existing images, and issues with end point devices. The RCS will not develop new images for use as this service is available as an option. The RCS does not include site visits. NTT DATA will be sole determiner of when the consulting requested is not within the scope of NTT DATA Workspace-as-a-Service RCS.

8. Images

8.1. NTT DATA recommends using the NTT DATA starter image provided with your Service for use in the NTT DATA Workspace environment.

8.2. Customer is advised that, as set out in further detail in the Exclusion below, converting images designed for the physical environments is extremely time-consuming and the results are usually less than optimal and that the Service (including RCS) will not support converting a Customer's physical image to the virtual environment nor the tools designed to do this conversion. NTT DATA has an optional Image Creation service available to help create your new virtual image.

9. Customer responsibilities

You will be responsible for the following activities:

9.1. Obtaining all licenses necessary in connection with the access and use, whether remotely or in-person with all software and applications subject to the Service, including Microsoft Windows Desktop operating system, Microsoft Virtual Desktop Access, Microsoft RDS CAL's and any application software;

9.2. Configuring and administering Active Directory;

9.3. Providing NTT DATA 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;

9.4. Provide computer accounts for Workspace-as-a-Service infrastructure;

9.5. Creating and removing user accounts for NTT DATA support personnel;

9.6. Assigning users to groups of virtual desktops, session desktops, and published applications via Active Directory;

9.7. Supporting end users, including, but not limited to client devices (desktops, notebooks, smartphones thin clients, etc.) and images (operating systems, applications and settings);

9.8. Creating and uploading desktop or server images;

9.9. Installing and maintaining the operating system and applications within the image;

9.10. Validating application compatibility in a virtual environment and monitoring application performance;

9.11. Performing backups of all existing data, software and programs on all affected systems prior to and during the delivery of this Service. Backup support may optionally be ordered and performed by NTT DATA;

9.12. Managing network connectivity and bandwidth from your network to end users and your network to the internet, including supporting the network hardware and software within your corporate network;

9.13. Complying with, and ensuring compliance by your end users with your company's professional use policies. Consult with your NTT DATA sales representative for further discussion regarding technical options as necessary;

9.14. Ensuring that Customer's authorized support contacts have purchasing authority to order/change Service;

9.15. Cooperating with and following the instructions given by NTT DATA phone analyst; Supporting Provisioning and any Service upgrade activities;

9.16. 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,

9.17. Complying with, and ensuring compliance by your end users with, the NTT DATA Cloud Solutions Agreement.

10. General Customer Obligations

10.1. Authority to Grant Access. Customer represents and warrants that it has obtained permission for both Customer and NTT DATA to access and use, whether remotely or in-person, Customer-owned or licensed software, hardware, systems, the data located thereon and all hardware and software components included therein, for the purpose of providing these Services. If Customer does not already have that permission, it is Customer's responsibility to obtain it, at Customer's expense, before Customer asks NTT DATA to perform these Services.

10.2. Customer Cooperation. Customer understands that without prompt and adequate cooperation, NTT DATA will not be able to perform the Service or, if performed, the Service may be materially altered or delayed. Accordingly, Customer will promptly and reasonably provide NTT DATA with all cooperation necessary for NTT DATA to perform the Service. If Customer does not provide reasonably adequate cooperation in accordance with the foregoing, NTT DATA will not be responsible for any failure to perform the Service and Customer will not be entitled to a refund.

10.3. Third Party Warranties. These Services may require NTT DATA to access hardware or software that is not manufactured by NTT DATA. Some manufacturers' warranties may become void if NTT DATA or anyone else other than the manufacturer works on the hardware or software. Customer will ensure that NTT DATA's performance of Services will not affect such warranties or, if it does, that the effect will be acceptable to Customer. NTT DATA does not take responsibility for third party warranties or for any effect that the Services may have on those warranties.

10.4. Best Practice Adoption for virtual desktop environment maintenance. Customer will follow industry best practices in developing and maintaining virtual desktop environment pool template images, desktop operating systems, and installed applications in order to provide a satisfactory end user experience. These practices include sufficient testing to verify the operation of virtual desktop pool template images prior to installation of new or changes to existing images. Pool template images should be reviewed at six month intervals. If Customer does not follow regular maintenance practices for pool templates, desktop operating systems, and applications NTT DATA will not be responsible for Service impacts to end users and Customer will not be entitled to a refund.

11. Exclusions

11.1. NTT DATA 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. Customer will complete a backup of all existing data, software and programs on all affected systems prior to and during the delivery of this Service. Customer should make regular backup copies of the data stored on all affected systems as a precaution against possible failures, alterations, or loss of data.

11.2. NTT DATA WILL HAVE NO LIABILITY FOR:

- ANY OF YOUR CONFIDENTIAL, PROPRIETARY OR PERSONAL INFORMATION;
- LOST OR CORRUPTED DATA, PROGRAMS OR SOFTWARE;

- DAMAGED OR LOST REMOVABLE MEDIA;
- THE LOSS OF USE OF A SYSTEM OR NETWORK; AND/OR
- FOR ANY ACTS OR OMISSIONS, INCLUDING NEGLIGENCE, BY NTT DATA OR A THIRD-PARTY SERVICE PROVIDER.

11.3. NTT DATA will not be responsible for the restoration or reinstallation of any programs or data.

11.4. NTT DATA Workspace-as-a-Service (including RCS) 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. NTT DATA Workspace-as-a-Service will not support any issues that arise as a result of the Customers providing a 'converted' image to use within the NTT DATA Workspace-as-a-Service environment. NTT DATA has an optional Image Creation service available to help create your new virtual image.

12. NTT DATA Responsibilities

Obtaining all licenses necessary to provide infrastructure in order to provide the Service, including, but not limited to, Microsoft Windows Server, hypervisor, and virtual desktop infrastructure (VDI) software licenses;

12.1. Notifying you to create or delete user accounts for NTT DATA support personnel;

12.2. Deploying desktop or server images provided by you;

12.3. Providing a starter image optimally configured for the NTT DATA Workspace environment;

12.4. Creating and removing desktops and application publications as well as managing required Group Policy Objects within the Customer provided Active Directory Organizational Unit;

12.5. Maintaining Service platform hardware and software that reside in NTT DATA data center, including connection from NTT DATA to the internet and the NTT DATA VPN concentrator;

12.6. NTT DATA will maintain backups of the Customer's environment and program data for the purpose of enabling the restoration of client Workspace-as-a-Service operations. This does not replace the Customer's backup responsibilities as noted in the Customer Responsibilities section. Performing incident and request management for platform-level support in accordance with Operational Response Targets in Appendix D; and,

12.7. Ensuring compliance with security statement in Appendix B.

13. Miscellaneous

13.1. No hardware is being transferred, sold, leased or licensed to Customer under this Service Description. To the extent NTT DATA uses hardware or software as part of its delivery of the Service, such hardware or software will be licensed, owned or otherwise held by NTT DATA. The Service can be hosted out of data centers in both the United States and the European Economic Area.

13.2. NTT DATA will perform an interview-based discovery process with Customer IT management in order to identify number of users, types of users, user locations, normal working hours, and associated requirements. During this discovery, Customer will select which region(s) to host the Service.

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

14. NTT DATA Services Terms & Conditions

14.1. This Service Description is entered between you and the NTT DATA entity identified on your invoice for the purchase of this Service. This Service is provided subject to and governed by Customer's separate signed master services agreement with NTT DATA that explicitly authorizes the sale of this Service. In the absence of such agreement, depending on Customer's location, this Service is provided subject to and governed by NTT DATA's Cloud Solutions Agreement (as applicable, the "Agreement") which can be accessed via the following link: https://www.nttdataservices.com/en-us/contracts.

14.2. Customer further agrees that by renewing, modifying, extending or continuing to utilize the Service beyond the initial term, the Service will be subject to the then-current Service Description available for review at https://www.nttdataservices.com/en-us/contracts.

14.3. To the extent that any terms of this Service Description conflict with any terms of the Agreement, the terms of this Service Description will prevail, but only to the extent of the specific conflict, and will not be read or deemed to replace any other terms in the Agreement which are not specifically contradicted by this Service Description.

14.4. By placing your order for the Services, receiving delivery of the Services, utilizing the Services or associated software or by clicking/checking the "I Agree" button or box or similar on the NTT DATAServices.com website in connection with your purchase or within a NTT DATA software or Internet interface, you agree to be bound by this Service Description and the agreements incorporated by reference herein. If you are entering this Service Description on behalf of a company or other legal entity, you represent that you have authority to bind such entity to this Service Description, in which case "you" or "Customer" shall refer to such entity. In addition to receiving this Service Description, Customers in certain countries may also be required to execute a signed Order Form.

15. Supplemental Terms & Conditions

15.1. Term of Service. This Service Description commences on the date listed on your Order Form and continues through the term ("Term") indicated on the Order Form. As applicable, the number of systems, licenses, installations, deployments, managed end points or end-users for which Customer has purchased any one or more Services, the rate or price, and the applicable Term for each Service is indicated on Customer's Order Form. Unless otherwise agreed in writing between NTT DATA and Customer, purchases of Services under this Service Description must be solely for Customer's own internal use and not for resale or service bureau purposes.

15.2. Important Additional Information

A. Payment for Hardware Purchased With Services. Unless otherwise agreed to in writing, payment for hardware shall in no case be contingent upon performance or delivery of cloud or SaaS services purchased with such hardware.
B. Optional Services. Optional services (including point-of–need support, installation, consulting, managed, professional, support, security or training services) may be available for purchase from NTT DATA and will vary by Customer location. Optional services may require a separate agreement with NTT DATA. In the absence of such agreement, optional services are provided pursuant to this Service Description.
C. Geographic Limitations and Relocation. This Service is not available at all locations. Service options, including service levels, technical support hours, and on-site response times will vary by geography and certain options may not be available for purchase in Customer's location, so please contact your sales representative for these details.

Appendix A: Pilot

The NTT DATA 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 sixty (60) days from Activation Date. This will include approximately fifteen (15) days for provisioning and the remainder for pilot environment use. The pilot may be extended in thirty (30)-day increments up to one hundred and twenty (120) day total pilot length (two (2) extensions).

The pilot will adhere to the terms and conditions of the NTT DATA Workspace-as-a-Service Service Description unless otherwise noted in this Appendix A.

1. 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 considered. Please consult with your NTT DATA representative for further guidance. Pilot profile desktop models reference in the following table, ex., “Standard”, are defined under “NTT DATA Workspace-as-a-Service components” on page two (2).

Profile (see table 1)	Standard	Enhanced	Professional	Premium
Maximum if one profile used on host	50	32	25	12
Profile Factor – multiply by number of seats desired – Total must be less than 50.	1	1.5	2	4
Application Delivery Host – Shared Session Desktops or Published Applications	Up to 4 shared session desktop/published application virtual machines (VMs). *Note*: Maximum concurrent user count will be dependent upon applications deployed.			

2. Billing

Billing as per the Service Description.

3. Provisioning

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

4. Exceptions to the full production Service Description

Pilots are intended for the Customer to test use cases, images and applications and NTT DATA response and support. Customers should not use the pilot NTT DATA 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

Appendix B: Security statement

Commitment to security

NTT DATA 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 centers, 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:[1]

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 datacenter 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.

Physical controls

NTT DATA's data centers are designed to support and protect mission-critical operations. These data centers provide multi-level physical security features and a rigidly-controlled operating environment to help protect Customer assets and operations. NTT DATA's service datacenters are audited annually to maintain ISO/IEC 27001 and other certifications.

[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 NTT DATA representative.

1. Access and Security Controls

   Access to NTT DATA's service datacenters is highly controlled. All entrances are monitored and have alarms for protection. These datacenters are staffed with 24-hour security officers to augment physical security features, providing protection of your operations.

2. CCTV Digital Recorders

   CCTV security cameras monitor designated sensitive areas.

3. Fire Suppression

   Industry standard fire suppression systems for multi-tenant datacenters are in use.

4. Environmental Controls

   NTT DATA's service data centers are constructed to meet the highest standards of redundancy. Service datacenters 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

1. Network and System Security

   Multiple levels of disparate defenses are used to protect customer information and strictly control network access to the NTT DATA data center. 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 NTT DATA datacenters 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 datacenter will be monitored from NTT DATA SecureWorks Security Operations Centers (SOC) located in the United States. NTT DATA subscribes to the provisions of Directive 95/46/EC for data privacy and protection.

2. 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 NTT DATA Workspace-as-a-Service firewalls.

3. Intrusion prevention systems

   NTT DATA 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.

4. Security Operations Center monitoring

   NTT DATA SecureWorks monitors all firewalls, web application firewalls and other network probes within the Service infrastructure to facilitate early detection of any attempted data breaches.

5. 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.

6. Vulnerability scanning

   Internal and external vulnerability scans are performed on NTT DATA's cloud infrastructure periodically and after any significant change in the network.

Administrative controls

1. Datacenter access history

   Physical access history to the NTT DATA datacenters is recorded.

2. Personnel security

   All NTT DATA employees with access to the Service environment are responsible for compliance with NTT DATA 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 NTT DATA's standard on Acceptable Use is displayed upon login to servers, desktops and notebooks. NTT DATA'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.

3. 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 NTT DATA Workspace-as-a-Service

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

NTT DATA will report Monthly Uptime Percentage on a Service wide basis which is inclusive of all production infrastructures and not for individual Customer environments. NTT DATA 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 NTT DATA 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 (as defined below), 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.

- **NTT DATA infrastructure**: The network and hardware infrastructure which extends from the Service computing resources to the data center-located router that provides the outside interface of each of NTT DATA's WAN connections to its backbone providers, in addition to the data center 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 NTT DATA 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 Excluded Minutes and Monthly Service Downtime. 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 or application delivery host subscriptions (includes file servers) for all Customers.

SLA Calculation:

Service based (Reported monthly & calculated by NTT DATA):

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

Credits

Provided 1) your account with NTT DATA is current and not suspended; and 2) NTT DATA's failure to meet this SLA was not a result from end-user over-subscription of an Application Delivery Host or under-sizing for any software or other technology you utilize with an Application Delivery Host, you may be eligible to receive the below-referenced credits ("Credits").

If NTT DATA does not meet the SLA for a particular calendar month during the term set forth in the Order Form, NTT DATA 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:

Monthly Uptime Percentage	Credit Percentage Amount
100% - 99.5%	0% of charges billed for the Service in month of occurrence
99.49% - 99.11%	10% of charges billed for the Service in month of occurrence
<= 99.10%	15% of charges billed for the Service in month of occurrence

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 = $\frac{100\ \text{X}\ (\text{Monthly Service Minutes} - \text{Monthly Service Downtime})}{\text{Monthly Service Minutes}}$

Therefore:

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

Incidents

Incidents are submitted through NTT DATA's incident management system.

Maximum credit

The maximum Credit available to Customer if NTT DATA is unable to meet the SLA is fifteen percent (15%) of the monthly fees for the calendar month of the occurrence. Any Credit that NTT DATA 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 NTT DATA, and all Credits will be based on NTT DATA'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 and 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 NTT DATA's sole liability, with respect to NTT DATA'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 NTT DATA's failure to achieve the SLA within thirty (30) days of the last date of the reported Monthly Service Downtime. The claim must include the incident ticket numbers reporting the failure. The claim must be sent by e-mail to the following address: NTTDATA_Cloud_SLA_Claims@NTTDATA.com. The e-mail must include the following information in a form provided by NTT DATA Workspace-as-a-Service on request:

- Customer name
- Customer account number, if applicable
- Name of the Service to which the claim relates, (e.g. NTT DATA 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 NTT DATA 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 NTT DATA 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. NTT DATA targets completion of these services at five (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 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

Incident Response Times	Severity Level 1 – 98% with 60 minutes Severity Level 2 – 98% within 60 minutes Severity Level 3 – 98% within 8 business hours Severity Level 4 – 98% within 16 business hours
Service Requests	Expand Pool (add VMs) – 8 business hours* New Pool – 24 business hours* Add HDD – <1TB total – 8 business hours Request Requiring new Host – 24 business hours This list is not inclusive of all request types. Other request response targets will be mutually determined based upon scope. * All requests target times assume no additional infrastructure (hosts) required. A request requiring 1 additional host will be satisfied within 24 business hours. Any larger capacity request will be project based effort.

Service Requests times are operational targets and are expected to support the normal operations of the NTT DATA 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 NTT DATA Workspace-as-a-Service Delivery in advance to prevent any delays caused by an excessive number of requests

Appendix E: Change Order Process

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 Form that has not been implemented or assigned a Service Start Date will not impact delivery dates for the original Order.

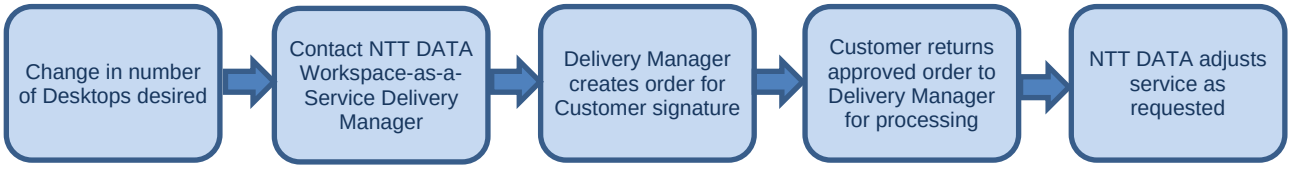
Examples of requests considered changes to the scope of Service requiring a change order:

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

Change Order Process

Customer determining need for additional services will contact the NTT DATA Workspace-as-a-Service delivery manager via the service desk. The NTT DATA Workspace-as-a-Service delivery manager will create on order based on your request and submit to you for approval. Customer will return the approved order to the NTT DATA 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 Operational Response Targets in this Service Description. Significant additions to service should be communicated to your NTT DATA Workspace-as-a-Service delivery manager as early as possible for planning purposes and to establish delivery expectations.



Billing

The Activation Date and Service Start Date 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 the Term. 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.

1. Non-Customer Impact

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

2. Moderate Customer Impact

   Maintenance that impacts Customer's Service availability for less than two (2) hours.

3. Significant Customer Impact

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

   Maintenance scheduling will be performed as follows:

4. Planned Maintenance

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

5. 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 NTT DATA so that proper information is distributed regarding the status of the Service environment and to coordinate any actions.

Customer will provide two (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:

Impact	Planned Maintenance	Unplanned/Urgent Maintenance
Non-Customer Impact	No Notice	No Notice
Moderate Customer Impact	2 weeks (10 business days)	ASAP not to exceed 1 hours
Significant Customer Impact	30 days	ASAP not to exceed 1 hours

Planned Maintenance

NTT DATA 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.

NTT DATA will normally adhere to the following maintenance windows for all countries where NTT DATA 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.

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. NTT DATA will normally communicate the schedule and scope of these events at least thirty (30) calendar days in advance in order to facilitate Customer planning and support. These events will usually need close communications between NTT DATA and the Customer. NTT DATA 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 NTT DATA's reasonable assessment, be scheduled at the next maintenance window, NTT DATA 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, NTT DATA 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 NTT DATA 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 NTT DATA 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 NTT DATA to follow Change Order Processes in accordance with Appendix E if such changes are to be supported. Any proposed change will be communicated to NTT DATA via a Service support request a minimum of two (2) weeks ten (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 NTT DATA to perform modifications to Service configuration, the Customer will call in an incident and NTT DATA will respond per the operational response targets in Appendix D.

NTT DATA 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 NTT DATA to make disclosures required by NTT DATA under NTT DATA's Services Provider License Agreement with Microsoft.

Appendix H: Technical Terms

This section will describe technical terminology referenced throughout this document.

- **Application Delivery Host**: the physical server that “Hosts” the virtual machines that deliver the session desktops, and applications utilized by users. The exact size and number of applications that can run per host is dependent upon the processing requirements and number of users of the application(s).
- **Starter Image**: a recommended gold image optimized for virtual desktop or application delivery. Gold images from physical desktop deployment should not be blindly transferred to virtual environments.
- **Desktop Pool**: a group of identical virtual desktops that are assigned to a user who has permissions to use the desktops. A single desktop cannot be used concurrently by multiple users. A user may or may not receive the same virtual desktop, depending upon how the pools and desktops assignments are defined, but will see their assigned applications and data storage regardless of desktop assignment.
- **Domain Organizational Unit**: a container or element within an Active Directory domain where users, groups, computers, and other organizational units are logically grouped. Containers may be established within a domain that represent the hierarchical and logical structures within an organization.
- **Gold Image**: a master template of a user’s virtual desktop and applications environment. Many users can share the same gold image. A gold image is used to configure the virtual machine that the user will access including the desktop operating system, accessible applications, and allocated storage space.