NTT DATA Dedicated Cloud (NDC)
Service Description

Version 7.0 | December 19, 2018

Table of Contents

Introduction 3
Shared and Dedicated Components 3
Virtual Machines 3
Networking 4
Storage 5
Security and Compliance 5
Service Delivery Management 9
Cloud Management Platform Service 10
Backup and Disaster Recovery 10
Other optional services 11
Service Management 11
Technical Support 11
Roles and Responsibilities Matrix 12
Exclusions 15
Billing and Contract Obligations 16
Requesting Changes to Dedicated Cloud 16
Additional Terms 17
Governing Agreement 18
Appendix A: Service level agreement for NTT DATA Dedicated Cloud 19
Appendix B: Key performance indicators for NTT DATA Dedicated Cloud 25
Appendix C: Reporting 26
Appendix D: HIPAA and HITECH 31
Appendix E: PCI DSS Framework 40
Appendix F: Dedicated Cloud Colocation Services 58
Appendix G: Cloud Backup service 63
Appendix H: Disaster Recovery (DR) Service 67
Appendix I : Cloud Management Platform Service 69
Appendix J: Dedicated Cloud Encryption Protection 73
Appendix K: Utility Zone service (Utility Zone) 76

Service Description

NTT DATA Dedicated Cloud

Introduction

NTT DATA Dedicated Cloud (“Dedicated Cloud”) is an infrastructure as a service (“IaaS”) offering designed to provide a secure private cloud environment, hosted and managed by NTT DATA Services, LLC (“NTT DATA”). Base service includes security, monitoring, support, and administration up to and including the hypervisor level for the compute, storage and network private cloud infrastructure used by the Dedicated Cloud within NTT DATA technology centers. Optional services are available at an additional charge.

The table below identifies infrastructure components that are dedicated to Client and components of the Dedicated Cloud that are shared between Client and NTT DATA’s other Clients.

Shared and Dedicated Components

Dedicated Components	Shared Components
Compute nodes	Physical data center network LAN
Virtual machine instances	Physical storage frames and SAN Fabric (Switches) to the logically separated LUNS
Virtual context firewall	
Storage LUNS inside storage frames	
Virtual load balancers (if purchased)	
VMware vCenter / Microsoft Hyper-V and Microsoft Virtual Machine Manager	

Virtual Machines

You as the Client can create, modify and decommission Virtual Machines (VMs) using self-service. NTT DATA will provide VM templates that can be used to create VMs, while you can also choose to import your own operating system (OS) images. NTT DATA VM templates cover most common guest operating systems, such as Microsoft Windows Server 2003, 2008, 2012 R2 and 2016, Red Hat Enterprise Linux, CentOS Linux and Ubuntu Server. Client is responsible for obtaining software

license rights for operating systems and any other software used in connection with the Dedicated Cloud other than software provided by NTT DATA.

Following licenses can be purchased from NTT DATA:

Microsoft Windows Server Operating System license	**Optional**
RedHat Enterprise Linux (RHEL) Operating System license	Optional**
Microsoft SQL Server license*	Optional**

*Microsoft SQL Server license does not include Windows Server Operating System license that needs to be purchased separately

**Due to licensing requirements, SQL or RHEL hosts must be in a separate SQL only or RHEL only cluster. SQL can also be purchased on individual VM level, in which case these restrictions do not apply.

Networking

NTT DATA supplies unmetered local area network ("LAN") access to the Client's hosts with low oversubscription of east-west communication in the datacenter fabric. NTT DATA's network infrastructure provides a secure and reliable environment for NTT DATA's Client's workloads and their external connectivity needs. The infrastructure includes a physical transport fabric and virtual networking components. Virtual network overlay technologies are used to provide each Client with an isolated network that can be deployed based on their unique requirements. NTT DATA provides Clients with an individual virtual switches, firewall, and virtual local area network ("VLAN"), to meet the segregation/isolation needs of each Client.

Dedicated Cloud offers following networking capabilities:

Public IP addresses	Optional
Internet – bandwidth	Optional
Site-to-Site VPN Managed Internet Protocol Security (IPSEC) VPN services providing site-to-site connectivity	Optional
Client VPN Clients can access their Dedicated Cloud environment remotely using secure and flexible SSL VPN	Optional
Software Defined Network Client's software defined network with multiple isolated tiers (e.g. application, database, and web).	Included
SDN Firewall SDN based virtual firewall, available as managed or self-service	Included
SDN Load Balancer (LB)	Optional

SDN based virtual load balancer, available as managed or self-service	
Advanced Load Balancing (LB) Advanced managed virtual load balancer suitable for internet facing or backend VM load balancing	Optional

Storage

Dedicated Cloud offers following storage tiers:

NAS Each NAS device contains 2 redundant controllers that are connected to the Client's network (10Gb) requiring 3 IPs in the LAN	**Optional**
Economy Storage Low cost storage provided as LUNs that is recommended for applications with lower storage performance requirements. Designed to deliver consistent baseline performance of 0.5 IOPS per GB and average latency of 1 ms (for 4 KB IOs) **Note, snapshots are not included.**	Optional
High Performance General Storage Read and write intensive SSD only storage provided as LUNs that is recommended for applications that need consistently very low latency. Designed to deliver consistent baseline performance of 3.0 IOPS per GB and average latency of 0.75 ms (for 4 KB IOs). Includes daily snapshots, maintained for a rolling 3-day period. Snapshots are taken at the LUN level (selection of individual files is not supported). **Note: Daily snapshot does not guarantee full recovery of data.**	Optional

Client is billed for Storage that is provisioned to Client VMs or used for VM Snapshots. NTT DATA will plan Storage datastores.

Security and Compliance

Commitment to Security

Dedicated Cloud is designed and built to address key security aspects, including:

- Integrity: Through Internet Protocol Security (IPsec) and Multiprotocol Label Switching (MPLS) connections, Dedicated Cloud provides industry standard encryption and message authentication to help prevent Client data from being modified during transmission.
- Confidentiality: Dedicated Cloud is designed to allow only authorized users (as nominated by the Client) to access information in their virtual environment using logical isolation and segmentation techniques for leveraged core network and storage components. Clients receive dedicated compute nodes. There is no multi-tenancy of Client workloads.

- Availability: Dedicated Cloud uses Uptime Institute Tier 3 or better data centers, and is built to minimize single points of failure. Robust system health monitoring tools are in place to pro-actively detect and remediate system issues or failures before they result in down time.

Dedicated Cloud may include the following Security and Compliance options:

Physical, Technical and Administrative controls (for hypervisor and below)	Included
Intrusion Detection Systems (IDS) Enterprise-grade intrusion detection systems (IDS) in place to inspect Dedicated Cloud infrastructure management networks to provide an additional mechanism for the early detection of data breaches.	Included
Dedicated Cloud Encryption Protection The Dedicated Cloud Encryption Protection solution protects data using strong encryption, privileged user access control and the collection of security intelligence logs. (See Appendix J for additional details)	Optional
HIPAA and HITECH Dedicated Cloud offers optional HIPAA & HITECH-compliant security and privacy controls that enable healthcare-sector Clients to host electronic protected health information (ePHI). For healthcare Clients, Appendix D includes a HIPAA matrix that lists NTT DATA's obligations and Client's obligations as part of the Business Associate Agreement also set forth in Appendix D.	Optional
PCI The Dedicated Cloud environment has been designed in accordance with the PCI DSS Level 1 Service Provider standard. (See Appendix E for additional details) PCI Clients may reference Appendix E for a PCI DSS Framework that provides a detailed explanation of the PCI DSS controls NTT DATA has implemented. The PCI DSS Framework also identifies any controls that remain exclusively the Client's responsibility. In many cases, NTT DATA and the Client will be responsible for the identified control, but, as indicated above, NTT DATA's responsibility ends with the hypervisor and Client must manage these controls within the context of its virtual data center environment.	Optional

Overview

Dedicated Cloud uses the following controls so that the integrity, confidentiality and availability of your information meets strong industry standards:

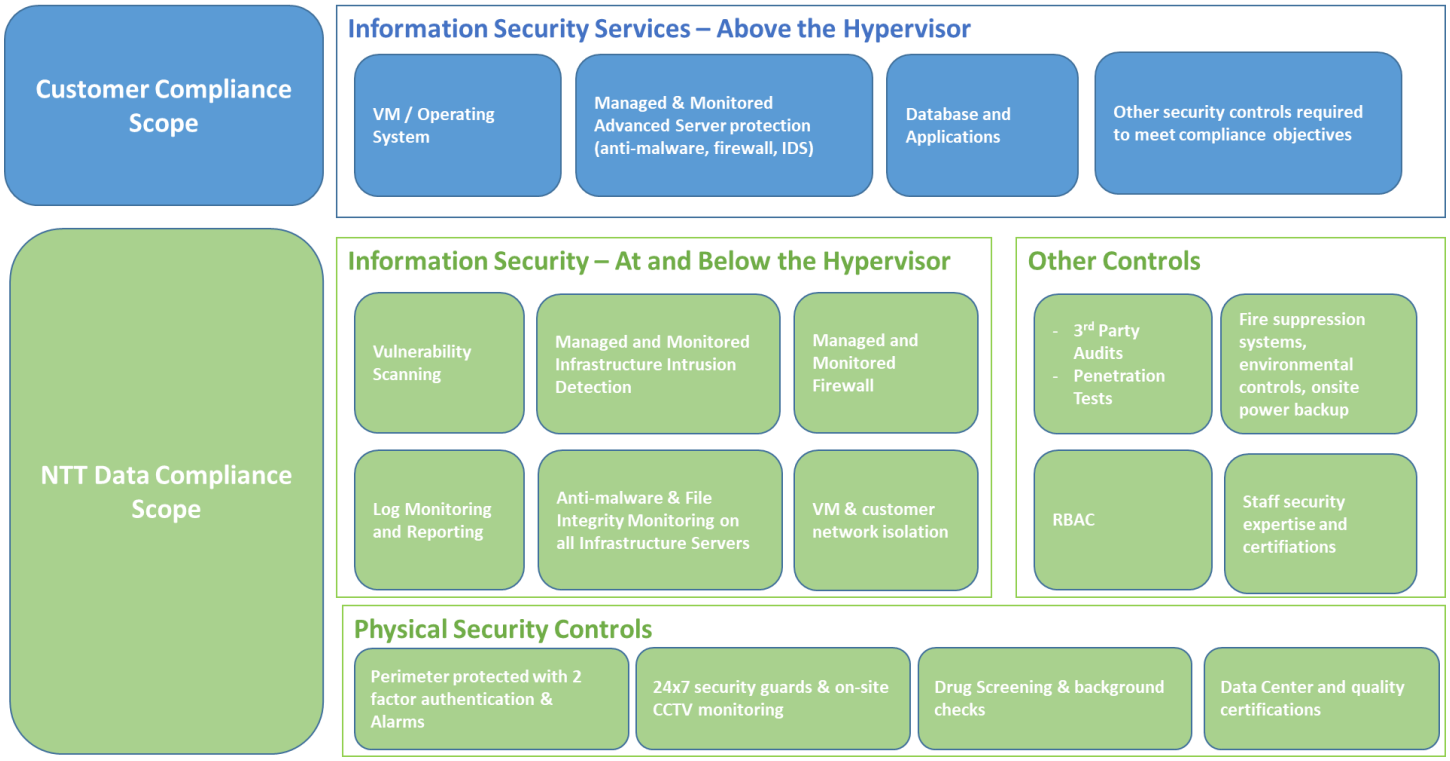
- **Physical controls**: Are countermeasures and environmental controls that affect the physical environment. Examples of physical controls are two-factor physical access controls, fire prevention systems, cooling systems, exit routes, security personnel and data center surveillance monitoring. A detailed description of physical controls is set out below.

- **Technical controls**: Also called logical controls and are countermeasures that rely upon use of technology to mitigate risk such as firewalls, anti-malware, ile integrity monitoring, intrusion detection systems, encryption mechanisms and automated compliance checks.
- **Administrative controls**: Are countermeasures that involve policy and procedures such as security and incident response policies, log audits, vulnerability scanning and penetration testing.

NTT DATA does not move Client data between data centers unless directed by the Client, however, NTT DATA proprietary information, including security logs and Dedicated Cloud monitoring and management information, may move between data centers and across international borders as necessary.

If additional services are provisioned into the environment outside of the scope of the services described in this Service Description, those additional services supply their respective security and compliance controls for those services.

NTT DATA security and compliance responsibilities extend from the data center floor up to and including the hypervisor. The Client is responsible for their own security and compliance controls and program above the hypervisor (unless these security services are separately contracted as an add-on service from NTT DATA), i.e. within the virtualized layer where the operating systems, databases, applications and integrations points reside. The below image illustrates this point.



Physical Controls

Service Data Centers are designed to support and protect mission-critical operations. These Data Centers provide multi-level physical security features and a rigidly-controlled physical environment to help protect Client assets and operations. Service Data Centers are audited annually to the SSAE 16 Type 2 standard and maintain ISO/IEC 27001:2013 certification as well as PCI DSS Certification for those datacenters hosting cardholder data.

ISO/IEC 27001:2013 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system for managing an organization's information security risks.

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

Technical Controls

- Network and System Security: Multiple levels of disparate defenses are used to protect Client information and to strictly control network access to the Data Center. Clients connect with Dedicated Cloud via IPsec, MPLS, and Dedicated Circuit connections to provide security and privacy of network transmissions, and to help prevent Client data from being modified during transmission. All access to Service servers is strictly monitored. In addition, Service servers are hardened to prevent intrusions and protect against day-to-day threats. The server hardware is selected and configured to maximize its reliability, security, scalability and efficiency.
- Firewalls: Clients receive virtual firewall context dedicated to protecting their virtual environment and is not shared with other tenants. All non-required firewall ports are blocked on Dedicated Cloud virtual firewalls by default, but Clients may customize their firewall configuration as-needed to meet their business and security needs.
- Intrusion Detection Systems: NTT DATA uses enterprise-grade intrusion detection systems (IDS) to monitor Dedicated Cloud infrastructure management networks and Client network traffic to provide another mechanism for the early detection of data breaches.
- Security Operations Center Monitoring: All Service infrastructure management components send system logs to a central log aggregation system. A dedicated NTT DATA Security Operations Center (SOC) monitors the system logs, as well as firewall and IDS events 24x7 to facilitate early detection of any attempted data breaches. NTT DATA Security Operations Center provides this industry leading capability to monitor and detect potential security incidents quickly and provide notification so that containment and remediation can begin minimizing the impact to Clients.

- Access Controls: Access to the Cloud Management Platform is restricted, based on the user's job function. To reduce the risk of misuse, intentional or otherwise, access is provided based on segregation of duties, least privileges, and need to know. Remote access to cloud management systems is restricted and requires two-factor authentication.
- Vulnerability Scanning and Penetration Testing: Internal and external vulnerability scans are performed on Dedicated Cloud infrastructure on a recurring basis. External and internal penetration tests, including network and in-depth application-layer penetration tests as well as testing of network isolation are performed at least annually and more frequently when changes to the environment mandate. The Client is not authorized to perform their own penetration testing against the NTT DATA infrastructure, but may perform penetration testing on their own VMs hosted in the Dedicated Cloud.

Administrative Controls

- Data Center Access History: Physical access history to the Data Centers is recorded.
- Personnel Security: All users with access to Dedicated Cloud environment are responsible for compliance with NTT DATA information security policies and standards. As part of NTT DATA's employment process, new employees undergo a screening process applicable as per local law. In the United States, personnel screening procedures include criminal background checks and drug screening.
- A banner stating the NTT DATA standard on Acceptable Use is displayed upon login to servers, desktops and notebooks. NTT DATA 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 NTT DATA-provided infrastructure and systems are managed by NTT DATA through a centralized change management program, which includes testing, back out procedures, business impact analysis and management approval, where appropriate.

Incident response procedures exist and are regularly tested to provide quick response to security and data protection incidents at the NTT DATA-provided infrastructure level. The procedures include incident analysis, containment, response, remediation, reporting and procedures for returning to normal operations.

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

Service Delivery Management

Service Delivery Management – Client Delivery Executive (CDE)	Optional

Governance of the Service is accomplished through a regular schedule of structured interactions between Client and NTT DATA which provide an avenue for escalation and a platform for issue identification, and resolution. NTT DATA will designate a Client Delivery Executive ("CDE") to manage overall service delivery and continuous improvement activities.

The CDE will:

- Work with the delivery and support team to identify opportunities and continually improve Client's experience with respect to their services
- Define key performance indicators and periodically review them with Client
- Advise Client of any high severity incidents, root causes, and resolution efforts for Dedicated Cloud
- Develop and review cloud plans with Client
- Manage the billing and invoicing process
- Provide a single point of contact for any Client escalations

Cloud Management Platform Service

Cloud Management Platform	Included

The Cloud Management Platform ("CMP") is a suite of capabilities that work across public, private, and hybrid cloud environments and provide Clients with management tools to centralize access management, service management and service optimization. The CMP is a service that is designed to shorten the time required, which may be from days to minutes, for provisioning new virtual resources and support of day 2 operations (open console, reboot, power on/off, snapshots, etc.) for the existing infrastructure, O/S layer, middleware, and applications. It is a high available multi-tenant service with a single installation in an NTT DATA datacenter in the US.

The management features within CMP include an intuitive user portal providing self-service tools, service catalog, provisioning, automation and workflow orchestration, usage metering and reporting, financial management tools, and workload optimization. External management APIs allow for custom integration/access.

The CMP enables Clients a single point with management and governance of access across public and private clouds. See Appendix I for additional details.

Backup and Disaster Recovery

Dedicated Cloud offers following Backup and Disaster Recovery options:

Cloud Backup service Provides local and second site backup capability. Available as self-service or fully-managed coverage levels. (See Appendix G for additional details)	**Optional**
Disaster Recovery (DR) service – self service	Optional

Provides second site DR capability in Data Centers ("Data Center(s)"). Supports mission critical workload replication between production and DR site along with Recovery Point Objectives (RPO) which may be as low as 30 mins. Service includes recovery site private cloud infrastructure, network connectivity to second site, and associated licensing fees. (See Appendix H for additional details)	

Other optional services

Dedicated Cloud Colocation services Provides secure, rack space for the hosting of rack mountable servers/devices in several regional Technology Centers in North America (NA). Racks are preconfigured to cross connect into the Dedicated Cloud to allow for network connectivity between the Client's servers/devices and Client's cloud environment. Rack space is sold in minimum increments of 5 rack units or full cabinets depending on the applicable datacenter locations Charges apply for racking, stacking and cabling as well as moves, adds, changes and deletes. (See Appendix F for additional details)	Optional
Utility Zone service Enables additional capacity of the Dedicated Cloud core infrastructure (compute and storage) without multi-month commitment. The Utility Zone service, when enabled, deploys to the same datacenter and network as Client's existing Dedicated Cloud infrastructure. The Utility Zone service is designed for non-persistent workloads and not recommended for persistent, storage-intensive workloads. (See Appendix K for additional details)	Optional

Service Management

Client will use NTT DATA's standard ITSM tool (provided during Onboarding) for all Service Management activities and follow NTT DATA's Service Management processes (unless these services are purchased under a separate NTT DATA service description or statement of work).

NTT DATA will provide service level management and reporting, as well as monitoring on the efficiency and effectiveness of the private cloud managed operations. NTT DATA will deliver the service management function across your private cloud environment, which establishes an organizational structure with well-defined roles and responsibilities. NTT DATA will assign process-oriented management roles to guide private cloud managed services standard operational processes and will provide metrics for any managed SLAs in line with ITIL best practices.

Technical Support

You may use the NTT DATA ITSM tool or contact the Service Desk via phone 24x7x365 for technical support. Client may assign up to 5 named contacts to contact the Service Desk on behalf of Client.

The Service Desk is a central point of contact for handling Client issues. Service Desk functions are comprised of the following:

- Log and route Client raised incidents to the cloud engineering or account assigned Client Delivery Executive (CDE)
- Provide assistance in raising service requests using the NTT DATA's ITSM tool
- Respond to inquiries around existing incidents or any service disruption statuses
- Route billing inquires to billing department and CDE

Support may be provided from outside of the country or region in which Client or Client's end users reside. Support is provided in English only.

Roles and Responsibilities Matrix

The following metrics and legends are used to define NTT DATA and Client responsibilities:

- "P" shall mean perform
- "H" shall mean help ("help" means assisting the other party in the performance of the applicable Task, as reasonably necessary and required)

General Section		
Activity	NTT DATA	Client
Support service enablement Onboarding activities: • **Provide environment requirements** • **Valid of configuration data and system integrations as applicable** • Provide Active Directory (AD) information for user access to CMP • Provide manager and user group role information for CMP • **Provide escalation and notification contacts** • **Provide sign-off to NTT DATA to confirm acceptance within 5 business days**		P
Support onboarding of Client to CMP services	P	
Provide timely access to Client resources if needed, including but not limited to, virtualization administrators and engineering, and project management		P
Provide, install and configure the Dedicated Cloud Infrastructure (including hypervisor and hardware)	P	
Provide hypervisor licensing for Dedicated Cloud	P	
Monitor the Dedicated Cloud Infrastructure	P	
Support and troubleshoot the Dedicated Cloud Infrastructure	P	

Schedule and communicate through the standard ITIL change management process (as specified by NTT DATA) Dedicated Cloud Infrastructure changes and maintenance	P	
Upgrade and patch the Dedicated Cloud Infrastructure	P	
Manage and maintain Data Center(s), racks, power and cooling	P	
Add Dedicated Cloud Infrastructure based on signed Change Order	P	
Remove Dedicated Cloud Infrastructure based on signed Change Orders	P	
Provide monthly Dedicated Cloud Infrastructure capacity reports upon request	P	
Capacity planning and forecasting for Client assigned Dedicated Cloud Infrastructure	H	P
Provide utilization and SLA reports upon request	P	
Manage Client's business continuity plan (unless NTT DATA has expressly agreed in writing and is explicitly contracted to design those services as a custom service)		P
CMP Specific Section		
Activity	**NTT DATA**	**Client**
Define Client organization in CMP	P	H
Assign appropriate managed systems to Client in the CMP	P	
Submit firewall rule access request for CMP	P	
Define access methods from Client to CMP		P
Define Client organization for manager and user group roles	P	H
Discovery of existing virtual servers and assigning owner names to each VM	P	H
Create new blueprints and templates (additional charge)	P	H
Customize existing blueprints and templates (additional charge)	P	H
Ongoing maintenance of blueprints and templates (additional charge)	P	H
Responsibility of 3rd party tools such as Chef/Puppet servers		P
Compute Specific Section		
Activity	**NTT DATA**	**Client**
Customize and harden of templates (if required)	P	H

Maintain customized and hardened templates	P	H
Provide licensing for all software and applications used for Dedicated Cloud other than software provided by NTT DATA		P
Virtual to virtual (V2V) conversions		P
Notify Client when cluster compute resources reach 75% utilization	P	
Maintain cluster compute resources under 85% utilization, by approving additional capacity or removing workloads		P
Modify and track changes to its dedicated virtual application environment		P
Application development and management, performance monitoring, database development and management (unless NTT DATA has expressly agreed in writing and is explicitly contracted to design those services as a custom service)		P
Provision and deprovision virtual servers in Client's virtual environment		P
Network Specific Section		
Activity	NTT DATA	Client
Define network subnets and IP space for Client's Dedicated Cloud environment		P
Assign and manage IPs inside subnets		P
Create network subnets and VLANs inside NTT DATA Dedicated Cloud Infrastructure upon request	P	H
Operate, maintain, and troubleshoot all physical and virtual network components residing in the Client's Dedicated Cloud Infrastructure	P	H
Provide SDN firewall	P	
Define and request firewall rules		P
Create and maintain firewall rules		P
Create and maintain firewall rules upon request (for managed firewalls only)	P	H
Define and request load balancer rules (if SDN LB or Advanced LB is purchased)		P
Create and maintain load balancer rules (if SDN LB or Advanced LB is purchased)		P
Create and maintain load balancer rules upon request (for SDN Managed LB or Advanced LB only)	P	H
Create and maintain Dedicated Cloud internal routing	P	
Provide managed VPN services for site-to-site connectivity over the internet (IPsec connections) (if purchased)	P	

Troubleshoot site-to-site VPN connections (if purchased)	P	P
Design and implement above hypervisor network security settings and requirements definitions (unless NTT DATA has expressly agreed in writing and is explicitly contracted to design those services as a custom service)		P
Storage Specific Section		
Activity	NTT DATA	Client
Provision storage from Dedicated Cloud arrays to host(s)	P	
Perform daily snapshots of eligible Cloud storage arrays and maintain copies for a rolling 3-day period	P	
Notify NTT DATA at least 30 calendar days in advance about planned increases in Provisioned Storage for more than 10 TB		P
Support backup/recovery requests from daily snapshot of Cloud Storage arrays, which may include additional costs to the Client to be agreed in advance and be subject to a separate agreement	P	
Security and Compliance Specific Section		
Activity	NTT DATA	Client
Monitor system logs up to and including the hypervisor level	P	
Monitor IDS events up to and including the hypervisor level	P	
Perform internal and external vulnerability scans on the Dedicated Cloud Infrastructure up to and including the hypervisor on a quarterly recurring basis	P	
Perform external and internal penetration tests annually on the Dedicated Cloud Infrastructure up to and including the hypervisor	P	
Audit annually to the SSAE 16 Type 2 standard	P	
Maintain ISO / IEC 27001:2005 certification	P	
Provide security management and access controls for in-service virtual servers and associated vLANsincluding Client software and data		P

Exclusions

For the avoidance of doubt, the following activities are not included in the scope of the Dedicated Cloud Service Description:

- Any services, tasks or activities other than those specifically noted in this Service Description.
- The development of any intellectual property created solely and specifically for the Client.

- Fixing or resolution of defects or malfunctions in third party software running in VMs encountered during the process of troubleshooting, resolving, patching, upgrading or maintenance.

Billing and Contract Obligations

Your Order Form will list the service options you have purchased. If purchased, such service options form part of your Dedicated Cloud. Billing for Dedicated Cloud is performed on a monthly basis in arrears and will include both fixed and variable costs.

Capacity additions (for example, adding an additional host) added within the last 7 days of the month will not be charged for the month in which the capacity is added. Client will be charged the full amount starting the next month. Capacity additions added prior to the last 7 days of the month will be charged the full, non-prorated rate for the month in which the capacity was added.

Dedicated Cloud is offered with a minimum one (1) year contract. At the end of the term, the Service will automatically be renewed for another year unless thirty (30) days prior written notice of your intent not to renew is provided to your NTT DATA account representative or CDE.

For billing-related questions, please email DL.CDE.NDC@nttdata.com.

Other add-on services:

- The Colo Service is billed monthly based on a minimum of a yearly commitment. Billing will commence the month installation services are complete. No monthly prorating of billing will be done. Rack space charges are billed in 5 RU increments. Network port charges are billed on a per port basis. One-time services, additional services, installation services and decommission services are billed in arrears following the month in which they occur. Client will be billed by NTT DATA, or will pay the service provider directly, for shipping of its equipment to the datacenter.

Requesting Changes to Dedicated Cloud

Clients may add/change their services with standard service catalog options or custom service capabilities through the Change Order process mentioned in the Order Form to request changes or additions to Dedicated Cloud. An Order Form signed by the Client or submitted by the Client as a self-service request through NTT DATA's ITSM tool is required to start implementing changes or additions to Dedicated Cloud.

Changes and Addition:

- Standard Service item addition(s)/change will be handled in 5 business days of the date of submission of a signed NTT DATA Change Order Form. This timeline will apply to changes or additions to storage, hosts, license, vLAN, VPN, firewall, as well as modifications to existing

data protection, modifications of existing Disaster Recovery, replication connectivity modifications, load balancing, modifications to credentials and compliance scope changes.

- Other changes to Dedicated Cloud outside of the scope of the paragraph above will be treated as projects and will be implemented based upon a mutually agreed schedule.
- Reductions in storage will be subject to Client freeing up the storage space before the storage decommissioning can commence.

Reducing dedicated host count or storage (in excess of 100Tb) from Service subscription is subject to the terms agreed on the NTT DATA Order Form and will require payment of subscription fees for the remainder of the term.

Additional Terms

1. The following will apply if Client is located in Canada or data is being transferred outside of US: Dedicated Cloud is provided from locations outside of Canada. In no event will NTT DATA be responsible or liable for determining whether Client is permitted to transmit, disclose, transfer, host or make available any data provided or transferred to, or accessed or hosted by NTT DATA from any location outside of Canada. All such responsibility for making such determination remain and reside with Client and any risk for any failures of Client to adhere to applicable privacy and data protection laws by transferring or disclosing data to NTT DATA under this Service Description remains exclusively with Client. Client is responsible for obtaining any third-party rights, permissions and consents or providing any notices to third parties as may be required. Client represents and warrants that it has obtained all rights, permissions, and consents necessary for NTT DATA to obtain, access, process, host, transfer, or otherwise use, as applicable, any Client provided or accessible data in accordance with this Service Description, including, without limitation, all applicable or necessary rights, permissions and consents.

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

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

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

5. Trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Specifications are correct at date of publication but are subject to change without notice at any time. NTT DATA and its affiliates cannot be responsible for errors or omissions in typography or photography.

Governing Agreement

This Service Description is governed by and subject to the terms and conditions in Client's master services agreement with NTT DATA to the extent such agreement explicitly authorizes Client to order Dedicated Cloud or, in the absence of such agreement, NTT DATA Cloud Solutions Agreement applies and is available on request or online at https://www.nttdataservices.com/en-us/contracts.

Appendix A: Service level agreement for NTT DATA Dedicated Cloud

The service levels and associated remedies described below apply to Dedicated Cloud when that Service is purchased directly from NTT DATA.

NTT DATA will follow a SLA based service delivery model. The source of alerts is either from the monitoring system or from user requests entered via the ticketing system, phone calls or e-mails.

- Resolution SLA timer is paused during the following ticket statuses: (a) “Waiting for Customer” (b) “On-Hold” (c) “Under Observation” (d) “Resolved”.
- Individual Client environments and processes influence service level compliances. In cases where the SLAs cannot be met, NTT DATA will publish those details during the pre-transition/planning phases.
- SLAs will be effective after 90 days of steady state operations or as agreed in writing during pre-transition phases.
- If Client does not implement NTT DATA recommendations for reducing alert and incident noise, service level commitments on those devices will not apply.

Availability SLA

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

NTT DATA will notify Client when total used virtual server cluster capacity and storage reaches 75% of purchased storage. Should total used storage exceed 85% of purchased storage, NTT DATA will not be liable for any failure to satisfy an Availability SLA target until total used storage returns to less than 85% of purchased storage.

Definitions: The following definitions apply to this Availability SLA.
“**Availability**” means Uptime divided by Scheduled Uptime multiplied by 100%. Availability is determined per the Monthly System Availability Reports. Availability is rounded to the nearest two-tenths of one percent.
“**Exceptions and Exclusions**” means (i) outages that occur during Maintenance Windows or during emergency maintenance windows (ii) outages attributable to a network carrier, (iii) failures attributable to the Client’s network, (iv) failures that result from changes to network circuits from Client location(s) to NTT DATA facilities that result in reduced bandwidth capacity for Dedicated Cloud, (v) failures attributable to a force majeure event, (vi) failures attributable to a breach of this Service Description by Client, (vii) failures attributable to the acts or omissions of the Client, a vendor or an entity to which Services are provided, (viii) Client exceeds 85% of virtual server cluster capacity, (ix) total used

storage exceeds 85% of purchased storage, or (x) failures that result from changes performed by Client self-service.

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

"**Uptime**" means the total number of minutes within any whole month that the Client's virtual servers are available for use by the Client. For clarity, Uptime will not be reduced as a result of any Exceptions and Exclusions.

Service Level Credits: If NTT DATA does not meet the Availability SLA for a particular month, NTT DATA will, at Client's request, provide the applicable remedy set out below ("Availability Credits").

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

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

Performance SLAs

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

Definitions: The following definitions apply to these Performance SLAs.

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

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

"**Resolution Time**" means the elapsed time between (i) the moment a service ticket is opened in the NTT DATA Service Management Workflow System, until (ii) the moment the service ticket is closed in accordance with the NTT DATA procedures manual because (A) the incident is resolved and Client

has not provided an accurate notification to NTT DATA that the incident has not been resolved; or (B) a temporary solution that addresses all of the material aspects of the incident (a "Workaround") is provided.

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

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

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

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

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

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

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

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

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

Incident Acknowledgement Time SLA

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

Data Capture	Incident records in the Service Management Workflow System are used to determine the total number of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents during a reporting period, the time each incident is received, and the elapsed time between submission of each Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incident in the Service Management Workflow System and the acceptance by a technician through the Service Management Workflow System of an assignment to address the incident.
Responsibility	
Reporting Period **Management Period**	Monthly Monthly
Service Metric	
Values	Metrics: Severity Level 1 Incident Acknowledgement Time – fifteen (15) minutes Severity Level 2 Incident Acknowledgement Time – thirty (30) minutes Severity Level 3 Incident Acknowledgement Time – eight (8) business hours Severity Level 4 Incident Acknowledgement Time – thirty-six (36) business hours
Minimum Service Level	In the aggregate, 95% or more of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents are acknowledged within, respectively, the Severity Level 1 Incident Acknowledgement Time, the Severity Level 2 Incident Acknowledgement Time, the Severity Level 3 Incident Acknowledgement Time and the Severity Level 4 Incident Acknowledgement Time.
Other	If NTT DATA fails to acknowledge an incident within the applicable minimum service level acknowledgement timeframe set forth above, but subsequently resolves such incident within the applicable minimum service level timeframe for incident resolution, NTT DATA may exclude the incident from its calculation of the minimum service level.
Calculation	(Number of total Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents acknowledged, respectively, within the Severity Level 1 Incident Acknowledgement Time, the Severity Level 2 Incident Acknowledgement Time, the Severity Level 3 Incident Acknowledgement Time and the Severity Level 4 Incident Acknowledgement Time divided by the total number of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents) * 100
Performance Credit	Severity Level 1 and Level 2 incidents are considered 'qualifying incidents' for Performance SLA evaluation, and are monitored and recorded by NTT DATA on a monthly basis. Clients are eligible to claim a Performance SLA credit in the amount of 2% of the total charges for the given month if total number of qualifying incidents recorded in the same month meets or exceeds 20. If 20 qualifying incidents do not occur in a particular month then these incidents are carried forward to subsequent month(s) until the cumulative count reaches 20. Once cumulative count of qualifying incidents reaches 20, Clients are eligible to claim a Performance SLA credit in the amount of 2% of the total charges for the last month over measured period.

Incident Resolution Time SLA

Objective	Measures the NTT DATA resolution time for the resolution of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents.
Method	
Data Capture	Incident tracking will be recorded and reported using Service Management Workflow System. Severity Level 1 and Severity Level 2 incidents are to be worked 24 hours a day, 7 days a week until Workaround or Services restoration is achieved.
Responsibility	
Reporting Period **Management Period**	Monthly Monthly
Service Metric	
Values	Metrics: Resolution Time – Severity Level 1 – four (4) hours Resolution Time – Severity Level 2 – eight (8) hours Resolution Time – Severity Level 3 – three (3) business day(s) Resolution Time – Severity Level 4 – ten (10) business day(s)
Exclusions	Resolution Time does not include the time that incident management tickets are in "suspend mode" because of hand-off to Client or Client's vendors. Service Requests are excluded from SLA calculations. Incidents determined to be within Client's responsibility to resolve are excluded from the calculations. Incidents determined to be caused by Client's implementation decisions that go against industry best practices and NTT DATA's implementation recommendation.
Minimum Service Level	In the aggregate, 95% or more of Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents are resolved within the applicable Resolution Times.
Calculation	(Number of total incidents at Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 closed within the applicable Resolution Time or properly downgraded by NTT DATA to a lower Severity Level within the applicable Resolution Time, divided by number of the total incidents at Severity Levels 1, 2, 3 and 4) * 100
Performance Credit	Severity Level 1 and Level 2 incidents are considered 'qualifying incidents' for Performance SLA evaluation, and are monitored and recorded by NTT DATA on a monthly basis. Clients are eligible to claim a Performance SLA credit in the amount of 2% of the total charges for the given month if total number of qualifying incidents recorded in the same month meets or exceeds 20. If 20 qualifying incidents do not occur in a particular month then these incidents are carried forward to subsequent month(s) until the cumulative count reaches 20. Once cumulative count of qualifying incidents reaches 20, Clients are eligible to claim a Performance SLA credit in the amount of 2% of the total charges for the last month over measured period.

Claim Procedures and Credit Limitations

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

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

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

Appendix B: Key performance indicators for NTT DATA Dedicated Cloud

The Key Performance Indicators ("KPIs") described below are for measurement and reporting purposes only, will be provided by NTT DATA on a commercially reasonable efforts basis and apply to Dedicated Cloud when Dedicated Cloud is purchased directly from NTT DATA. Any failure on the part of NTT DATA to satisfy the below-listed KPIs will not entitle Client to claim any credit or claim any other remedy. Unless otherwise noted herein, the definitions set forth in Appendix A apply to this Appendix B.

Root Cause Analysis KPI

Objective	Report and track root cause analysis relating to the NTT DATA infrastructure in accordance with the NTT DATA problem management procedures.
Method	
Data Capture	Problem tracking will be recorded and reported using the Service Management Workflow System.
Responsibility	
Reporting Period **Management Period**	Monthly Monthly
Service Metric	
Minimum Service Level	In the aggregate, 90% or more of Severity Level 1 incidents and Severity Level 2 incidents (at Client's request) are subjected to a root cause analysis and are submitted to Client for review within ten (10) business days of the later of (i) the Severity Level 1 incident moving to "Service Restored" status, or (ii) as to Severity Level 2 incidents only, Client's request for a root cause analysis being entered in the Service Management Workflow System.
Calculation	(Number of Severity Level 1 and Severity Level 2 incidents subjected to a root cause analysis and submitted to Client for review within the minimum service level divided by total number of Severity Level 1 incidents and Severity Level 2 incidents for which Client requests a root cause analysis) * 100

Appendix C: Reporting

The Cloud Management Platform (CMP) (as further described in Appendix I) has a self-service reporting capability allowing for a report to be run once or scheduled to run on a regular frequency (ex. daily, weekly, monthly). The report can be viewed from within the Service Portal and can be sent via email to one or more recipients. The report filtering categories are Virtual Machines, Virtual Services, Service Requests, and Software. Within the categories there are many subcategories types and multiple filters can be used allowing for granular reporting on specific information. Reports created by a user are specific to them and available to you in any organization you are authorized to access within the CMP.

The diagram below provides the categories and subcategories of filters available to create reports

Virtual Machines	**Virtual Services**	**Service Requests**	**Software**
Configuration	**Configuration**	Approvers	Identifying Number
Availability Set	# VMs	Assigned To	Install Date
Connected Media	DNS Name	Category	Install Location
Connection State	IP Address	Date Completed	Install State
Customizable OS	Name	Date Submitted	Name
Hardware Version	Power State	Days Inactive	Package Cache
Highly Available	Product	Duration	VM Name
Instance Type	Product URL	ID	Vendor
Name	Vendor	Required By	Version
Power State	Version	State	
Root Device Type	**Cost**	Submitted By	
Running Status (Guest Tools)	Annual Cost	Target Service	
Status (Guest Tools)	Daily Cost	Type	
Type	Monthly Cost	Waiting On	
Version (Guest Tools)	Quarterly Cost		
Version Status (Guest Tools)	Weekly Cost		
Cost	**Custom Attributes**		
Annual Cost	Billing Model		
Daily Cost	Billing Status		
Monthly Cost	Cost Center		
Quarterly Cost	Data Center Location		
Weekly Cost	ICPR Number		
Custom Attributes	PCI Applicable		
Billing Model	Primary Application		
Billing Status	Project Code		
Cost Center	Project ID		
Data Center Location	SLA		
ICPR Number	SOX Applicable		
PCI Applicable	Service Type		

Primary Application	Task ID		
Project Code	aka Name		
Project ID	**Lifecycle**		
SLA	Created By		
SOX Applicable	Date Created		
Service Type	Expiry Date		
Task ID	Expiry State		
aka Name	In Service Catalog		
Guest OS Details	**Ownership**		
Applications	All Owner Emails		
Guest OS	All Owner Logins		
Hot Fixes	All Owner Names		
Last Guest OS Scan	IT Contact Email		
Last Logon Time	IT Contact Login		
Last Logon User	IT Contact Name		
OS Details	Primary Owner Email		
Services	Primary Owner Login		
Infrastructure	Primary Owner Name		
Last Performance Update			
Virtual Service Parent			
Lifecycle			
Created By			
Date Created			
Expiry Date			
Expiry Extensions Remaining			
Expiry State			
Last Deployed			
Maintenance Group			
Power Schedule Group			
Powered Off Since			
Service Request			
Uptime			
Operational			
Approval State			
Compliance Issue			
Compliance State			
End of Life State			

Ownership			
All Owner Emails			
All Owner Logins			
All Owner Names			
IT Contact Email			
IT Contact Login			
IT Contact Name			
Primary Owner Email			
Primary Owner Login			
Primary Owner Name			
Recommendations			
Has Recommendations			
Recommendation Annual Cost Savings			
Recommendations Instance Type Down			
Recommendations Instance Type Up			
Recommended CPU Change			
Recommended Memory Change (GB)			
Rightsizing Group			
Resources - CPU			
CPU Count			
CPU Limit (GHz)			
CPU Shares			
CPU Shares Level			
Reserved CPU (GHz)			
CPU Ready Daily Avg (%)			
CPU Ready Daily Peak (%)			
CPU Ready Weekly Avg (%)			
CPU Ready Weekly Peak (%)			
CPU Usage Daily Avg (%)			
CPU Usage Daily Avg (MHz)			
CPU Usage Daily Peak (%)			
CPU Usage Daily Peak (MHz)			
CPU Usage Weekly Avg (%)			
CPU Usage Weekly Avg (MHz)			
CPU Usage Weekly Peak (%)			
CPU Usage Weekly Peak (MHz)			
Resources - Memory			
Memory (GB)			
Memory Limit (GB)			

Memory Shares			
Memory Shares Level			
Reserved Memory (GB)			
Static Memory			
Memory Ballooning Daily Avg (MB)			
Memory Ballooning Daily Peak (MB)			
Memory Ballooning Weekly Avg (MB)			
Memory Ballooning Weekly Peak (MB)			
Memory Consumed Daily Avg (MB)			
Memory Consumed Daily Peak (MB)			
Memory Consumed Weekly Avg (MB)			
Memory Consumed Weekly Peak (MB)			
Memory Overhead Daily Avg (MB)			
Memory Overhead Daily Peak (MB)			
Memory Overhead Weekly Avg (MB)			
Memory Overhead Weekly Peak (MB)			
Memory Swap In Daily Avg (MB/s)			
Memory Swap In Daily Peak (MB/s)			
Memory Swap In Weekly Avg (MB/s)			
Memory Swap In Weekly Peak (MB/s)			
Memory Swap Out Daily Avg (MB/s)			
Memory Swap Out Daily Peak (MB/s)			
Memory Swap Out Weekly Avg (MB/s)			
Memory Swap Out Weekly Peak (MB/s)			
Memory Usage Daily Avg (%)			
Memory Usage Daily Peak (%)			
Memory Usage Weekly Avg (%)			
Memory Usage Weekly Peak (%)			
Resources - Network			
DNS Name			
IP Address			
MAC Address			
Network Usage Daily Avg (MB/s)			
Network Usage Daily Peak (MB/s)			
Network Usage Weekly Avg (MB/s)			
Network Usage Weekly Peak (MB/s)			
Resources - Storage			
Disk Provisioning Type			
Free Disk Space (%)			

Free Disk Space (GB)			
Logical Disk Size (GB)			
Oldest Snapshot Date			
Oldest Snapshot Name			
Physical Disk Size (GB)			
Provisioned Storage (GB)			
Snapshot Count			
Unallocated Disk Space (GB)			
Unpartitioned Disk Space (GB)			
Used Storage (GB)			
Virtual Disk Size (GB)			
Virtual Disk Size Scanned (GB)			
NAS Tier Usage (GB)			
SAN Performance - Compellent Tier Usage (GB)			
SAN Standard - Compellent Tier Usage (GB)			
SSD SAN Performance - Pure Tier Usage (GB)			
SSD SAN Standard - Pure Tier Usage (GB)			
Storage Tier 6 Tier Usage (GB)			
Undefined Tier Usage (GB)			
Disk Usage Daily Avg (MB/s)			
Disk Usage Daily Peak (MB/s)			
Disk Usage Weekly Avg (MB/s)			
Disk Usage Weekly Peak (MB/s)			
Max Latency Daily Avg (ms)			
Max Latency Daily Peak (ms)			
Max Latency Weekly Avg (ms)			
Max Latency Weekly Peak (ms)			

Appendix D: HIPAA and HITECH

Business Associate Agreement for NTT DATA Dedicated Cloud

This Business Associate Agreement ("BAA") applies to Dedicated Cloud when HIPAA-compliant services are applicable and purchased directly from NTT DATA as an optional add-on service to the NTT DATA Dedicated Cloud. This BAA shall commence on the Activation Date and shall automatically terminate on the expiration or termination of Dedicated Cloud.

1. Section References and Definitions. Any reference to a section in this Appendix shall mean a section of this Appendix, unless expressly set forth otherwise in such reference. The following definitions shall serve to define certain of the capitalized terms used within this Appendix. Other capitalized terms used in this Appendix are defined in the Agreement. Capitalized terms not otherwise defined below or in the Agreement shall have the meanings given to them in HIPAA and are incorporated herein by reference, including, but not limited to: Breach, Compliance Date, Data Aggregation, Electronic Protected Health Information, Individual, Protected Health Information, Required by Law, Secretary, Security Incident, and Unsecured Protected Health Information.

1.1. "Breach Notification Provisions" means the "Notification in the Case of Breach of Unsecured Protected Health Information" provisions under HIPAA as contained in 45 C.F.R. Part 164, subpart D.

1.2. "Business Associate" means, for purposes of this Appendix, NTT DATA Services, LLC.

1.3. "Controlled" and its derivatives means the legal, beneficial or equitable ownership, directly or indirectly, of more than fifty percent (50%) of the capital stock (or other ownership interest, if not a corporation) of such entity ordinarily having voting rights.

1.4. "Covered Entity" means, for purpose of this Appendix, the Client specified on the Order Form.

1.5. "Covered Entity Systems" has the meaning set forth in Section 3.2.2.

1.6. "Designated Record Set" means a "designated record set" (as such term is defined in 45 C.F.R. § 164.501) containing PHI that is being maintained by Business Associate (or its Workforce or Subcontractors).

1.7. "Discovery" means discovery as described in 45 C.F.R. § 164.410(a)(2).

1.8. "Electronic PHI" means PHI that is Electronic Protected Health Information.

1.9. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996.

1.10. "PHI" means Protected Health Information created, received, maintained or transmitted by Business Associate (or its Workforce or Subcontractors) from or on behalf of Covered Entity or its Affiliates.

1.11. "Privacy Rule" means the federal standards for the "Privacy of Individually Identifiable Health Information" under HIPAA as contained in 45 C.F.R. Part 160, subpart A and Part 164, subparts A and E.

1.12. "Security Regulations" means the federal "Security Standards for the Protection of Electronic Protected Health Information" under HIPAA as contained in 45 C.F.R. Part 160, subpart A and Part 164, subparts A and C.

1.13. "Subcontractor" means a "subcontractor" (as such term is defined in 45 C.F.R. § 160.103) of Business Associate (excluding Affiliates of Business Associate) who creates, receives, maintains or transmits PHI on behalf of Business Associate.

1.14. "Unsecured PHI" means PHI that is Unsecured Protected Health Information.

1.15. "Workforce" means "Workforce" (as such term is defined in 45 C.F.R. § 160.103) members of Business Associate who create, receive, maintain or transmit PHI on behalf of Business Associate.

2. Permitted and Required Uses and Disclosures of PHI.

2.1. Business Associate is permitted to use and disclose PHI (a) to perform functions, activities and the Services for, or on behalf of, Covered Entity as required to perform Business Associate's obligations in the Agreement; (b) as Required by Law; and (c) as otherwise permitted in this Appendix; provided, however, Business Associate may not use or disclose PHI in a manner that would violate the requirements of the Privacy Rule if done by Covered Entity, except as provided in Sections 2.2 – 2.4.

2.2. Business Associate is permitted to use PHI if necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

2.3. Business Associate is permitted to disclose PHI if necessary for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate if (a) the disclosure is Required by Law; or (b) Business Associate obtains reasonable written assurances from the person to whom it disclosed the PHI that it will remain confidential and used or further disclosed only as Required by Law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

2.4. Business Associate is permitted to use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B) if Data Aggregation services are necessary for Business Associate to perform its obligations under the Agreement or Covered Entity otherwise requests Data Aggregation services from Business Associate.

2.5. Business Associate is permitted to disclose PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. § 164.502(j)(1).

3. Business Associate's Obligations.

3.1. Restriction on Uses and Disclosures. Business Associate will use and disclose PHI only as permitted or required by this Appendix.

3.2. Safeguards.

3.2.1. Subject to Sections 3.2.2 below, Business Associate shall (a) use appropriate safeguards as required by the Privacy Rule to prevent the use or disclosure of PHI other than as permitted by the Agreement or this Appendix; and (b) with respect to Electronic PHI, use appropriate safeguards and comply, where applicable, with subpart C of HIPAA to prevent the use or disclosure of Electronic PHI other than as

permitted by this Appendix, including complying with each of the requirements of 45 C.F.R. Sections 164.306, 164.308, 164.310, 164.312, and 164.316 as applicable to business associates.

3.2.2. When Business Associate is present at a facility of Covered Entity or its Affiliates or is accessing or utilizing equipment, software, tools, network components or other information technology owned, leased or licensed by Covered Entity or its Affiliates ("**Covered Entity Systems**"), Business Associate will comply with Covered Entity's standard safeguards to prevent the use or disclosure of PHI (including Covered Entity's standard administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of Electronic PHI) applicable to such Covered Entity facility or such Covered Entity System, provided Covered Entity has given Business Associate prior notice of such safeguards in writing or in the same manner as Covered Entity provides notice of such safeguards to its own employees and other contractors. Business Associate is not responsible for (a) implementing safeguards with respect to the facilities of Covered Entity or its Affiliates or the Covered Entity Systems; or (b) providing or implementing upgrades, modifications or changes to, or replacements of, any Covered Entity Systems, in each case, that are required to comply with HIPAA or other state or federal privacy and security laws or regulations, except to the extent the Agreement expressly provides that Business Associate has any such responsibilities.

3.2.3. Notwithstanding the provisions of Sections 3.2.1 and 3.2.2, Table 1 below (**"HIPAA Safeguard Responsibility Matrix"**) contains express provisions in which Covered Entity and Business Associate have allocated security and privacy responsibilities between them, including allocating the responsibility for the types of security safeguards that are governed by the Security Regulations. If there is a conflict between such provisions in the Table and the provisions of Section 3.2.1 or Section 3.2.2, such provisions in the Table shall control.

3.3. Reporting. Business Associate will report to Covered Entity (a) any use or disclosure of PHI by it or its Workforce or Subcontractors in violation of Business Associate's obligations in this Appendix of which it becomes aware; and (b) any Security Incident of which it becomes aware. With respect to unsuccessful Security Incidents, the significant number of meaningless attempts to access Business Associate's systems and data, including Electronic PHI, makes it impossible for Business Associate to report such unsuccessful Security Incidents in real-time or on any regular basis. Accordingly, the Parties agree that Business Associate is not required to report unsuccessful Security Incidents, whether occurring now or in the future, when they do not result in actual unauthorized access, use, disclosure, modification or destruction of Electronic PHI or interference with an information system that contains or processes Electronic PHI, such as but not limited to the following: (i) pings on the firewall; (ii) attempts to logon to a system, device or database with an invalid password or user name; (iii) denial of service attacks; and (iv) port scans.

In addition, Business Associate will, following Business Associate's Discovery of a Breach of Unsecured PHI, notify Covered Entity of such Breach in accordance with 45 C.F.R. § 164.410 of the Breach Notification Provisions.

3.4. Business Associate's Subcontractors. Business Associate shall require that each Subcontractor agrees in writing to provide reasonable assurances that such Subcontractor will comply with restrictions and conditions that are substantially similar in all material respects to the restrictions and conditions that apply to Business Associate under this Appendix with respect to such PHI. Notwithstanding the foregoing, Business Associate will treat its Affiliates who create, receive, maintain or transmit PHI as members of its Workforce and will not be required to obtain such written assurances from such Affiliates, and Business Associate will be responsible for any actions of such Affiliates in violation of Business Associate's obligations in this Appendix.

3.5. Access to PHI in Designated Record Sets. Upon Business Associate's receipt of a written request from Covered Entity for access to PHI about an Individual contained in any Designated Record Set(s), Business Associate will make available to Covered Entity, or to the Individual if so instructed by Covered

Entity, such Designated Record Set(s) in the format and on the media in use by Business Associate as of the date of the request in order for Covered Entity to meet its obligations to make the PHI available in accordance with 45 C.F.R. § 164.524. If specifically requested by Covered Entity in such written request or other written notice, Business Associate will (i) provide such PHI in a format, or on media, that is different than that in use by Business Associate as of the date of such request or notice, and/or (ii) transmit copies of such Electronic PHI in an electronic format directly to the person designated in such notice or request or make copies of such PHI in a paper form and provide such copies to the person designated in such notice, provided Covered Entity shall reimburse Business Associate for the applicable reasonable costs incurred by Business Associate in complying with such notice or request. If an Individual requests access to PHI directly from Business Associate, Business Associate will promptly forward such request to Covered Entity.

3.6. Amendment of PHI in Designated Record Sets. Upon Business Associate's receipt of a written request from Covered Entity for an amendment to PHI about an Individual contained in any Designated Record Set(s), Business Associate will make available to Covered Entity such Designated Record Set(s) in the format and on the media in use by Business Associate as of the date of the request in order for Covered Entity to meet its obligations to amend PHI in accordance with 45 C.F.R. § 164.526. To the extent Business Associate has an obligation under the Agreement to make amendments to PHI contained in any Designated Record Set(s), upon Business Associate's receipt of a written request from Covered Entity for an amendment to any such PHI, Business Associate shall make amendments to such PHI as instructed by Covered Entity in such request in order for Covered Entity to meet its obligations to amend the PHI in accordance with 45 C.F.R. § 164.526. If an Individual request an amendment to PHI directly from Business Associate, Business Associate will promptly forward such request to Covered Entity.

3.7. Documentation of Disclosures. Business Associate will document disclosures of PHI made by it or its Workforce or Subcontractors and information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of such disclosures in accordance with 45 C.F.R. § 164.528; provided, however, with respect to such disclosures that are made (a) as part of the provision of Services; or (b) at Covered Entity's request, unless the Agreement expressly provides that Business Associate has the financial responsibility to provide the equipment, software, tools or other information technology necessary to track and document the disclosures referenced in clauses (a) and (b), Covered Entity will either (i) be responsible for providing such equipment, software, tools or other information technology; or (ii) allow Business Associate to track such disclosures utilizing a system Covered Entity uses to track disclosures made by Covered Entity that are required to be tracked under 45 CFR § 164.528. Upon Business Associate's receipt of written notice from Covered Entity that Covered Entity has received a request for an accounting of disclosures of PHI regarding an Individual, Business Associate will make available to Covered Entity the information collected by it in accordance with the foregoing to permit Covered Entity to respond to such request in accordance with 45 C.F.R. § 164.528. In the event the request for an accounting is delivered directly to Business Associate, Business Associate will promptly forward such request to Covered Entity.

3.8. Covered Entity Obligations under the Privacy Rule. To the extent the Business Associate is to carry out a Covered Entity obligation under the Privacy Rule as part of its obligations under the Agreement, Business Associate will comply with the requirements of the HIPAA Privacy Rule that apply to Covered Entity in the performance of such obligation; provided, however, this Section 3.8 is not intended to, and does not, limit or change any of the other agreed upon provisions in this Appendix, and if there is a conflict between this Section 3.8 and any other agreed upon provision in this Appendix, such agreed upon provision shall prevail and control.

3.9. Disclosure to the Secretary. Business Associate will make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA, subject to any applicable legal privileges. Business Associate will notify Covered Entity upon its receipt of any such request for access by the Secretary and provide Covered Entity with a copy of such request.

3.10. Mitigation. Business Associate will mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI by it or its Workforce or Subcontractors in violation of Business Associate's obligations in this Appendix.

3.11. Minimum Necessary. When using, requesting or disclosing PHI, Business Associate shall make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the request, use or disclosure.

3.12. Prohibition on Sale of PHI. Business Associate shall not directly or indirectly receive remuneration in exchange for a disclosure of PHI in violation of 45 C.F.R. § 164.502(a)(5)(ii), unless Covered Entity has provided Business Associate with a valid authorization from the Individual in accordance with 45 C.F.R. § 164.508(a)(4).

3.13. Compliance with Notices. Upon Business Associate's receipt of a notice from Covered Entity under Section 4.2, Business Associate will promptly (a) cease the use and disclosure of any such Individual's PHI as specified in the notice; (b) comply with the limitations specified in the notice; and/or (c) comply with the restrictions specified in the notice, as applicable. To the extent compliance with such notice(s) interferes with, delays, hinders or precludes Business Associate's ability to perform its obligations set forth in the Agreement, Business Associate will be excused from, and relieved of liability for, any such non-performance.

4. Covered Entity's Obligations.

4.1. Consents, Authorizations and Permissions. Covered Entity agrees to obtain and maintain such consents, authorizations and/or permissions, if any, as may be necessary or required under HIPAA or other local, state or federal laws or regulations to permit Covered Entity to disclose PHI to Business Associate in order for Business Associate to use and disclose PHI as required or permitted under this Appendix.

4.2. Notices. Covered Entity agrees to notify Business Associate in writing of (a) of any modifications to, restrictions on, defects in, or revocation or other termination of effectiveness of, any consent, authorization or permission referenced in Section 4.1; (b) any limitation(s) in its notice of privacy practices; and (c) any restriction(s) to the use or disclosure of PHI with which Covered Entity has agreed, to the extent any such modifications, defects, revocations, limitations or restrictions affect Business Associate's permitted or required uses and disclosures of PHI specified in this Appendix.

4.3. Requested Uses and Disclosures. Without limiting Sections 2.2 – 2.4, Covered Entity agrees it will not request, and the performance of Business Associate's obligations under the Agreement will not require, Business Associate to use or disclose PHI in any manner that would not be permissible if done by Covered Entity.

4.4. Other Business Associates. If Business Associate is required in order to perform its obligations in the Agreement, or if Business Associate is otherwise instructed by Covered Entity, to disclose PHI to other business associates (as defined in HIPAA) of Covered Entity or its Affiliates, or to disclose PHI to any other entities or persons, when it is Required by Law to obtain from such business associates, entities or persons a business associate agreement, confidentiality agreement or other type of nondisclosure agreement, except as expressly provided in Section 2.3 or Section 3.4 of this Appendix, Covered Entity will be responsible for obtaining such agreements with such business associates, entities or persons.

5. Termination.

5.1. Termination for Cause by Covered Entity. Upon Covered Entity's knowledge of a material breach of Business Associate's obligations in this Appendix by Business Associate or its Workforce or Subcontractors, Covered Entity may (a) terminate the Agreement (including this Appendix) by providing Business Associate prior written notice if Business Associate fails to cure such breach within thirty (30) days of its receipt of written notice from Covered Entity specifying the nature of such breach; (b) immediately terminate the Agreement (including this Appendix) by providing Business Associate prior written notice if a cure of such breach is not possible; or (c) report such breach to the Secretary if termination of the Agreement is not feasible.

5.2. Effect of Termination.

5.2.1. Except as provided in Section 5.2.2 below, upon the termination of this Appendix for any reason, (a) Business Associate will return or destroy all PHI in the possession of Business Associate or its Workforce or Subcontractors; and (b) Business Associate and its Workforce and Subcontractors will not retain copies of such PHI.

5.2.2. In the event returning or destroying such PHI is infeasible, (a) Business Associate will provide to Covered Entity notification of the conditions that make return or destruction infeasible; and (b) for so long as such PHI is maintained by Business Associate or its Workforce or Subcontractors, Business Associate will extend the protections of this Appendix to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible.

6. Miscellaneous.

6.1. Amendments to Comply with Law. If (a) any final amendments to HIPAA are enacted after the Effective Date; or (b) any final amendments to other data security and privacy laws are enacted after the Effective Date, to the extent such amendments require modifications to the then-current compliance obligations of Covered Entity or Business Associate under this Appendix, Covered Entity and Business Associate agree to promptly meet and negotiate in good faith to mutually agree on such modifications. Any material modifications to Business Associate's obligations under this Appendix may include changes in financial terms as reasonably required to support such cost of compliance.

6.2. Regulatory References. A reference in this Appendix to a section of HIPAA means the section in effect as of the Effective Date.

6.3. Survival.

6.3.1. Business Associate's rights and obligations under Section 5.2.2 of this Appendix will survive the termination of this Appendix until Business Associate no longer retains such PHI and such PHI has been returned to Covered Entity or destroyed.

6.3.2. Business Associate's rights and obligations under Section 3.9 of this Appendix will survive the termination of this Appendix.

6.3.3. For each disclosure of PHI made by Business Associate or its Workforce or Subcontractors subject to an accounting under Section 3.7, except for such disclosures where the information collected in

accordance with Section 3.7 is contained in Covered Entity systems as described in Section 3.7, if the information collected in accordance with Section 3.7 has not been provided to Covered Entity by the termination of this Appendix, Business Associate's obligations under Section 3.7 for each such disclosure will survive the termination of this Appendix until the earlier to occur of (a) six (6) years after such disclosure, or (b) the date the information collected by Business Associate in accordance with Section 3.7 is provided to Covered Entity.

6.3.4. With respect to PHI retained by Business Associate after the termination of this Appendix pursuant to Section 5.2.2, Covered Entity's obligations under Section 4 of this Appendix will survive the termination of this Appendix until Business Associate no longer retains such PHI.

6.4. No Third-Party Beneficiaries. Except as expressly provided in this Appendix, nothing in this Appendix is intended to confer, nor will anything herein confer, upon any person or entity other than the Parties hereto any rights, remedies, obligations or liabilities whatsoever.

6.5. Interpretation.

6.5.1. Except as expressly provided in this Appendix, if there is any conflict between the terms of this Appendix and the terms of the Agreement with respect to the matters covered in this Appendix, the terms of this Appendix will control.

6.5.2. Any ambiguity in the terms of this Appendix will be resolved to permit Covered Entity and Business Associate to comply with HIPAA, subject to the mutual agreement of Business Associate and Covered Entity if any such interpretation results in a material change in the obligations of Covered Entity or Business Associate under the Agreement (including this Appendix).

HIPAA Safeguard Responsibility Matrix

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

	Maintenance records (A)		✓
Workstation use	Workstation use (R)	✓	✓
Workstation security	Workstation security (R)	✓	✓
Device and media controls	Media disposal (R)		✓
	Media re-use (R)		✓
	Accountability (A)		✓
	Data backup and storage (A)	✓	✓
Standards	Implementation Specifications	✓	✓
Technical Safeguards			
Access control	Unique user identification (R)	✓	✓
	Emergency access procedure (R)	✓	✓
	Automatic logoff (A)	✓	✓
	Encryption and decryption (A)	✓	
Integrity	Mechanism to authenticate ePHI (A)	✓	
Person or entity authentication	Person or entity authentication (R)	✓	
Transmission security	Integrity controls (A)	✓	
	Encryption (A)	✓	

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

Appendix E: PCI DSS Framework

The PCI DSS framework service is an optional add-on service to the NTT Dedicated Cloud. The PCI Security Standards Council offers standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to provide the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a payment card data security process, including detection and appropriate reaction to security incidents.

All organizations processing credit card information, regardless of their deployment model, are required to be certified. For larger merchants (Merchant Level 1 is the largest type), validation by an independent and approved reviewer is required. A PCI Qualified Security Assessor (QSA) is authorized to perform an independent assessment and certify a vendor.

NTT DATA has implemented the PCI DSS framework and has been validated as a Level 1 Service Provider. A validated service provider is one that has undergone an audit by an independent QSA and is found to be in conformity with the PCI security standards outlined in the latest version of the Data Security Standard.

The chart below represents the NTT DATA Dedicated Cloud's PCI DSS controls framework and clearly delineates the responsibilities of NTT DATA and the Client.

Meeting PCI Compliance Requirements with Cloud Infrastructure Management - This matrix explains the responsibilities assigned to each party when the Dedicated Cloud service model is used to support workloads regulated by PCI DSS 3.2		
Dedicated Cloud - Base IaaS Service		
Responsible Entity • NTT DATA - NTT DATA is solely responsible • Both - Client is responsible for this control on system components they manage. NTT DATA is responsible for implementing this control on the hypervisor and all Cloud infrastructure system components not managed by the Client. • Client - Client is solely responsible		**Notes**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
1.1 Establish firewall and router configuration standards that include the following: 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	Both	
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Both	
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	Both	
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Both	
1.1.5 Description of groups, roles, and responsibilities for management of network components	NTT DATA	

1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Both	
1.1.7 Requirement to review firewall and router rule sets at least every six months	Both	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Both	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Both	
1.2.2 Secure and synchronize router configuration files.	NTT DATA	
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Both	NTT DATA does not permit wireless networking in the Cloud environment. Clients must ensure a firewall exists between any wireless access points they manage, and their in-scope cloud resources.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Both	
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Both	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	Both	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	Both	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Both	
1.3.5 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)	NTT DATA	
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Both	
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.	Both	NTT DATA manages Client firewalls at their specific direction.
1.4 Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: · Specific configuration settings are defined for personal firewall software. · Personal firewall software is actively running. · Personal firewall software is not alterable by users of mobile and/or employee-owned devices.	Both	
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Both	

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	Both	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Both	
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: · Center for Internet Security (CIS) · International Organization for Standardization (ISO) · SysAdmin Audit Network Security (SANS) Institute · National Institute of Standards Technology (NIST).	Both	
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server.	Both	
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Both	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure**.**	Both	
2.2.4 Configure system security parameters to prevent misuse.	Both	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Both	
2.3 Encrypt all non-console administrative access using strong cryptography.	Both	
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Both	
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Both	
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	NTT DATA	
Requirement 3: Protect stored cardholder data		
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: · Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements · Processes for secure deletion of data when no longer needed ·Specific retention requirements for cardholder data	Both	The Client specifies data retention requirements for cardholder data stored on their virtual machines. Where backup services are purchased, NTT DATA is responsible for retaining backups of CHD

· A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.		in accordance with Client requirements.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: - There is a business justification and - The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	Client	
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	Client	
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	Client	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Client	
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.	Client	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: · One-way hashes based on strong cryptography, (hash must be of the entire PAN) · Truncation (hashing cannot be used to replace the truncated segment of PAN) · Index tokens and pads (pads must be securely stored) · Strong cryptography with associated key-management processes and procedures.	Client	
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts	Client	
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:	Client	
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: - Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date - Description of the key usage for each key - Inventory of any HSMs and other SCDs used for key management	N/A	N/A – Cloud IaaS Personnell do not support Client encryption. Note: if encryption support is included in the overall solution (in addition to IaaS), the encryption controls in this

		section may become a responsibility of NTT DATA
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	Client	
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: - Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key - Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) - As at least two full-length key components or key shares, in accordance with an industry-accepted method	Client	
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	Client	
3.6.1 Generation of strong cryptographic keys	Client	
3.6.2 Secure cryptographic key distribution	Client	
3.6.3 Secure cryptographic key storage	Client	
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	Client	
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	Client	
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.	Client	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	Client	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Client	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Client	
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use.	Both	NTT DATA is responsible for assisting with the configuration of VPN connectivity. All other cardholder data encryption in transit is the responsibility of the Client.

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	N/A	NTT DATA does not permit wireless networking in the Cloud environment.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	Client	
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Client	
Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs.		
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Both	
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Both	
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Both	
5.2 Ensure that all anti-virus mechanisms are maintained as follows: · Are kept current, · Perform periodic scans · Generate audit logs which are retained per PCI DSS Requirement 10.7.	Both	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Both	
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Both	
Requirement 6: Develop and maintain secure systems and applications.		
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	Both	
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Both	
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: · In accordance with PCI DSS (for example, secure authentication and logging) · Based on industry standards and/or best practices. · Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.	Client	NTT DATA IaaS solution does not utilize custom-developed software – controls specific to application development are N/A

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to Clients.	Both	
6.3.2 Review custom code prior to release to production or Clients in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: · Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. · Code reviews ensure code is developed according to secure coding guidelines · Appropriate corrections are implemented prior to release. · Code-review results are reviewed and approved by management prior to release.	Client	
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	Both	
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls	Both	
6.4.2 Separation of duties between development/test and production environments	Both	
6.4.3 Production data (live PANs) are not used for testing or development	Client	
6.4.4 Removal of test data and accounts before production systems become active / goes into production.	Both	
6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:	Both	
6.4.5.1 Documentation of impact	Both	
6.4.5.2 Documented change approval by authorized parties	Both	
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system	Both	
6.4.5.4 Back-out procedures	Both	
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Both	
6.5 Address common coding vulnerabilities in software-development processes as follows: · Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory · Develop applications based on secure coding guidelines	Both	
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Both	
6.5.2 Buffer overflows	Both	
6.5.3 Insecure cryptographic storage	Both	
6.5.4 Insecure communications	Both	
6.5.5 Improper error handling	Both	
6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)	Both	
6.5.7 Cross-site scripting (XSS)	Both	

6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions)	Both	
6.5.9 Cross-site request forgery (CSRF)	Both	
6.5.10 Broken authentication and session management	Both	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: · Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes	Both	
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties	Both	
Requirement 7: Restrict access to cardholder data by business need to know		
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access	Both	
7.1.1 Define access needs for each role, including: · System components and data resources that each role needs to access for their job function · Level of privilege required (for example, user, administrator, etc.) for accessing resources	Both	
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities	Both	
7.1.3 Assign access based on individual personnel's job classification and function	Both	
7.1.4 Require documented approval by authorized parties specifying required privileges	Both	
7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	Both	
7.2.1 Coverage of all system components	Both	
7.2.2 Assignment of privileges to individuals based on job classification and function	Both	
7.2.3 Default "deny-all" setting	Both	
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties	Both	
Requirement 8: Identify and authenticate access to system components		
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	Both	
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data	Both	
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects	Both	
8.1.3 Immediately revoke access for any terminated users	Both	
8.1.4 Remove/disable inactive user accounts within 90 days	Both	

8.1.5 Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: · Enabled only during the time period needed and disabled when not in use · Monitored when in use	Both	
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts	Both	
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID	Both	
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session	Both	
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: · Something you know, such as a password or passphrase · Something you have, such as a token device or smart card · Something you are, such as a biometric	Both	
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components	Both	
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys	Both	
8.2.3 Passwords/phrases must meet the following: · Require a minimum length of at least seven characters. · Contain both numeric and alphabetic characters Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above	Both	
8.2.4 Change user passwords/passphrases at least once every 90 days	Both	
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used	Both	
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use	Both	
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Both	
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Both	
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	Both	
8.4 Document and communicate authentication procedures and policies to all users including: · Guidance on selecting strong authentication credentials · Guidance for how users should protect their authentication credentials · Instructions not to reuse previously used passwords · Instructions to change passwords if there is any suspicion the password could be compromised	Both	

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: · Generic user IDs are disabled or removed. · Shared user IDs do not exist for system administration and other critical functions · Shared and generic user IDs are not used to administer any system components	Both	
8.5.1 Additional requirement for service providers only: Service providers with remote access to Client premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each Client.	NTT DATA	
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: · Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts · Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	Both	
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: · All user access to, user queries of, and user actions on databases are through programmatic methods · Only database administrators have the ability to directly access or query databases · Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)	Client	
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Both	
Requirement 9: Restrict physical access to cardholder data		
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	NTT DATA	
9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	NTT DATA	
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	NTT DATA	
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	NTT DATA	
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: - Identifying onsite personnel and visitors (for example, assigning badges) - Changes to access requirements	NTT DATA	

- Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)		
9.3 Control physical access for onsite personnel to the sensitive areas as follows: · Access must be authorized and based on individual job function · Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled	NTT DATA	
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	NTT DATA	
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained	NTT DATA	
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel	NTT DATA	
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration	NTT DATA	
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	NTT DATA	
9.5 Physically secure all media	NTT DATA	
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	NTT DATA	
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	NTT DATA	
9.6.1 Classify media so the sensitivity of the data can be determined	NTT DATA	
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked	NTT DATA	
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals)	NTT DATA	
9.7 Maintain strict control over the storage and accessibility of media	NTT DATA	
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually	NTT DATA	
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	NTT DATA	
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	NTT DATA	
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed	NTT DATA	
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution	Client	

9.9.1 Maintain an up-to-date list of devices. The list should include the following: · Make, model of device · Location of device (for example, the address of the site or facility where the device is located) · Device serial number or other method of unique identification.	Both	
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	Client	
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: · Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. · Do not install, replace, or return devices without verification. · Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). · Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Client	
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties	NTT DATA	
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 Implement audit trails to link all access to system components to each individual user	Both	
10.2 Implement automated audit trails for all system components to reconstruct the following events:	Both	
10.2.1 All individual user accesses to cardholder data	Both	
10.2.2 All actions taken by any individual with root or administrative privileges	Both	
10.2.3 Access to all audit trails	Both	
10.2.4 Invalid logical access attempts	Both	
10.2 5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Both	
10.2.6 Initialization, stopping, or pausing of the audit logs	Both	
10.2.7 Creation and deletion of system-level objects	Both	
10.3 Record at least the following audit trail entries for all system components for each event:	Both	
10.3.1 User identification	Both	
10.3.2 Type of event	Both	
10.3.3 Date and time	Both	
10.3.4 Success or failure indication	Both	
10.3.5 Origination of event	Both	
10.3.6 Identity or name of affected data, system component, or resource	Both	

10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Both	
10.4.1 Critical systems have the correct and consistent time.	Both	
10.4.2 Time data is protected.	Both	
10.4.3 Time settings are received from industry-accepted time sources.	Both	
10.5 Secure audit trails so they cannot be altered.	Both	
10.5.1 Limit viewing of audit trails to those with a job-related need.	Both	
10.5.2 Protect audit trail files from unauthorized modifications.	Both	
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Both	
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Both	
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Both	
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.	Both	
10.6.1 Review the following at least daily: - All security events - Logs of all system components that store, process, or transmit CHD and/or SAD - Logs of all critical system components - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems (IDS), authentication servers, e-commerce redirection servers, etc.).	Both	
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Both	
10.6.3 Follow up exceptions and anomalies identified during the review process.	Both	
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Both	
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: - Firewalls - IDS/IPS - FIM - Anti-virus - Physical access controls - Logical access controls - Audit logging mechanisms - Segmentation controls (if used)	NTT DATA	
10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:	NTT DATA	

- Restoring security functions - Identifying and documenting the duration (date and time start to end) of the security failure - Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause - Identifying and addressing any security issues that arose during the failure - Performing a risk assessment to determine whether further actions are required as a result of the security failure - Implementing controls to prevent cause of failure from reoccurring - Resuming monitoring of security controls		
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Both	
Requirement 11: Regularly test security systems and processes.		
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	NTT DATA	
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	NTT DATA	
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	NTT DATA	
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Both	
11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	Both	
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	Both	
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	Both	
11.3 Implement a methodology for penetration testing that includes the following: · Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) · Includes coverage for the entire CDE perimeter and critical systems · Includes testing from both inside and outside the network · Includes testing to validate any segmentation and scope-reduction controls · Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 · Defines network-layer penetration tests to include components that support network functions as well as operating systems · Includes review and consideration of threats and vulnerabilities experienced in the last 12 months	Both	

· Specifies retention of penetration testing results and remediation activities results.		
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Both	
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Both	
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Both	
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Both	
11.3.4.1 *Additional requirement for service providers only*: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	NTT DATA	
11.4 Use intrusion-detection techniques to detect intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection engine, baselines, and signatures up to date.	Both	
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Both	
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	Both	
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Both	
Requirement 12: Maintain a policy that addresses information security for all personnel.		
12.1 Establish, publish, maintain, and disseminate a security policy.	Both	
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	Both	
12.2 Implement a risk-assessment process that: · Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),	Both	

· Identifies critical assets, threats, and vulnerabilities, and · Results in a formal documented analysis of risk.		
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	Both	
12.3.1 Explicit approval by authorized parties	Both	
12.3.2 Authentication for use of the technology	Both	
12.3.3 A list of all such devices and personnel with access	Both	
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Both	
12.3.5 Acceptable uses of the technology	Both	
12.3.6 Acceptable network locations for the technologies	Both	
12.3.7 List of company-approved products	Both	
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Both	
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	Both	
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	Client	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Both	
12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: - Overall accountability for maintaining PCI DSS compliance - Defining a charter for a PCI DSS compliance program and communication to executive management	Both	
12.5 Assign to an individual or team the following information security management responsibilities:	Both	
12.5.1 Establish, document, and distribute security policies and procedures.	Both	
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Both	
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Both	
12.5.4 Administer user accounts, including additions, deletions, and modifications.	Both	
12.5.5 Monitor and control all access to data.	Both	
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	Both	
12.6.1 Educate personnel upon hire and at least annually.	Both	

12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Both	
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	Both	
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	Both	
12.8.1 Maintain a list of service providers	Both	
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the Client, or to the extent that they could impact the security of the Client's cardholder data environment.	Both	
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Both	
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Both	
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	NTT DATA	
12.9 Additional requirement for service providers only: Service providers acknowledge in writing to Clients that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the Client, or to the extent that they could impact the security of the Client's cardholder data environment.	NTT DATA	
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	Both	
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: · Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum · Specific incident response procedures · Business recovery and continuity procedures · Data backup processes · Analysis of legal requirements for reporting compromises · Coverage and responses of all critical system components · Reference or inclusion of incident response procedures from the payment brands.	Both	
12.10.2 Test the plan at least annually.	Both	
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Both	
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	Both	
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, firewalls, and file-integrity monitoring systems.	Both	
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Both	

12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: - Daily log reviews - Firewall rule-set reviews - Applying configuration standards to new systems - Responding to security alerts - Change management processes		
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: - Documenting results of the reviews - Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program		
Requirement A.1: Shared hosting providers must protect the cardholder data environment		
A.1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS.	NTT DATA	
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.	NTT DATA	
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.	NTT DATA	
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	Both	NTT DATA cannot ensure logging and audit trails are enabled within the Client's virtual environment - this remains a Client responsibility. NTT DATA is responsible for logging and audit trails on system components within the cloud infrastructure.
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	Both	

Appendix F: Dedicated Cloud Colocation Services

Dedicated Cloud Colocation Services is an optional add-on service to NTT DATA Dedicated Cloud. NTT DATA provides Colocation Services in the following centers in North America (NA):

- Plano Technology Center (PTC), Texas
- Western Technology Center (WTC), Washington/Quincy
- Florence Technology Center (FTC), Kentucky
- Cincinnati Technology Center (CTC), Ohio

1. Dedicated Cloud Colocation Services – PTC, FTC and WTC

Introduction to Dedicated Cloud Colocation Services

Dedicated Cloud Clients that purchase Dedicated Cloud Colocation Services ("Colo Service(s)") have access to a leveraged rack space for the hosting of server processing platforms. One-time provisioning services for electrical power connection, network cable connection and server installation must be purchased in connection with Client's purchase of Colo Services.

Offer Description

The Dedicated Cloud Colo Service is a supplementary service intended to provide the Client with rack space, power, cooling and physical security for Client's equipment and power cables as defined in more detail below in section called Equipment Criteria (the "Equipment") shipped to and hosted by NTT DATA within a Data Center with internetworking to Client's Dedicated Cloud instance(s). This Colo Service requires, but is not limited to, the following high-level process steps:

- Client configures Equipment with IP addresses from Client assigned pool of addresses from the Dedicated Cloud
- Client ships Equipment, and necessary peripherals as outlined below, to Data Center
- NTT DATA receives Equipment and installs in a Data Center rack
- Power and network cables are run to Equipment in the rack
- Equipment is connected with network connectivity to Client's Dedicated Cloud environment
- NTT DATA personnel power up Equipment and notify Client when Equipment is available
- For an additional one-time fee, following termination or expiration of the Colo Service contract, NTT DATA will decommission remote access, uninstall Equipment and ship Equipment to Client at Client-provided shipping address

As reasonably necessary, NTT DATA will assist Client to resolve local Equipment issues with vendor access to equipment at Data Center. Client agrees that Client and not NTT DATA is the owner of and responsible for its data and for compliance with any laws or regulations applicable to its data. NTT DATA strongly advises use of encryption on Client Equipment utilized for the Colo Service to reduce risks of data compromise during shipment.

Equipment Criteria

Equipment's supported by NTT DATA for this Colo Service only include devises between 1 U and 4 U configurations. NTT DATA does not support equipment which is a tower, blade or enterprise servers in the Colo Service.

Client-supplied Equipment must meet the following criteria:

- Current consumption 3A-32A
- Have 120VAC or 240VAC compatible power supplies
- Physical dimensions will not exceed:
  - 19” (depth) x 1.75” (width) x 25.5” (height) for 1U-3U equipment
  - 19” (depth) x 1.75” (width) x 26.4” (height) for 4U-5U equipment
  - a maximum weight of 200lbs

If Client equipment does not meet these specified requirements or if Client provides its equipment to NTT DATA in a condition such that NTT DATA is unable, as a technical matter, to provide the Colo Service, NTT DATA will return equipment to Client at Client’s specified shipping address, at Client’s cost.

Service Offer

Colo Services consist of:

- Leveraged rack space that is ready-to-populate. Rack space is purchased in 5 rack unit (RU) increments and includes connectivity for out of band Client equipment access, infrastructure, and air-flow space.
- Electrical power consists of:
  - Dual power receptacles
  - Power types options available are: 17.2kW-8.6.kW effective rating; 208/110V,30A (100% rated); and 3-Phase,5-wire WYE (3P+N+E)
- 1Gb/10Gb Ethernet network ports and shared network switches between Client’s equipment and the Dedicated Cloud environment.
- Keyboard Video Monitor (KVM) connect access to physical components in Colo Data Centers to manage remotely without having to access the Data Center.

Colo Facilities and Equipment Services consists of the following:

- NTT DATA will provide the facilities and Colo Services in the applicable NTT DATA or Partner data center based in the applicable region as advised by NTT DATA.
- The Data Center facility is air-conditioned with secure raised floor space.
- NTT DATA will coordinate with Client for management of installation and maintenance of Client’s Equipment.

Additional Dedicated Cloud Colo Service details and options available at an additional charge are listed below.

Service Details
One-time services • Cabling network connections from Client Equipment to the Dedicated Cloud environment which can be done for single or redundant network connections. • Colocation electrical connections if Client Equipment only has one power connection; there is an additional charge for an electrical transfer switch for Clients with multiple power connections. • Requests for move/add/change/decommissions and configuration changes are submitted as an additional service via the NTT DATA service desk and will result in additional fees.

Installation Services • Electrical power connection, network cable connection, fiber cable connection and Equipment installation are not included in the space or electrical power rates under the Colo Service, but are available as one-time installation services. Electrical power connection includes the preparation and installation of electrical power to a cabinet, rack or other data center floor location. This service also provides electrical receptacles and all electrical power wiring needed to connect the rack and Equipment to the data center electrical power distribution units (PDUs). Charges are incurred on a per receptacle basis. • Network cable installation includes the preparation and installation of CAT6 network cabling from the data center network switches to the Client Equipment. This service also includes patch panel ports and all patch cables required for installation. Charges are incurred on a per run basis. • Fibre cable installation includes the preparation and installation of fiber cable from a network switch/SAN to the server location. Charges are incurred on a per run basis. • Equipment installation includes the preparation and installation of the server into a designated cabinet. Charges are incurred on a per server basis. • NTT DATA will receive Client Equipment at the specified Data Center. • NTT DATA will provide port availability and cabling services for out of band management of Colo devised (Integrated lights out (iLO)/NTT DATA Remote access card iDRAC).
Recurring charges • Smart Hands – billed hourly as needed for any moves, adds or changes required by the Client, including configuration changes and cable moves after install or reboots

2. Dedicated Cloud Colocation Services – Full Cabinets - WTC, CTC

Introduction to Dedicated Cloud Colocation Services

Clients that purchase Colo Services, will have access to full cabinets for rack mountable devices, and floor space for self-standing equipment. One-time installation services for electrical power connections, network and/or fiber cable connections and racking devices are included in the standard service charge for Colo Services to the Client.

Offer Description

The Colo Service is a supplementary service intended to provide Clients with floor space, power, cooling and physical security for Client's infrastructure hosted by NTT DATA. This Colo Service requires, but is not limited to, the following process steps:

- Client ships Equipment, and necessary peripherals as outlined below, to Data Center
- NTT DATA receives and installs Equipment in a Data Center
- Power and network/fiber cables are connected to Equipment in the cabinet(s)
- Equipment is connected to Client's location with Client provided network circuits or NTT DATA Internet bandwidth
- NTT DATA personnel power up Equipment and notify Client when Equipment is available
- For an additional one-time fee, following termination or expiration of the Colo Service contract, NTT DATA will decommission remote access, uninstall Equipment and ship Equipment to Client at Client-provided shipping address

As necessary, NTT DATA will assist Client to resolve local Equipment issues with vendor access to devices at the Data Center. Client agrees that Client and not NTT DATA is the owner of and responsible for its data and for compliance with any laws or regulations applicable to its data. NTT DATA strongly advises use of strong encryption on Client Equipment utilized for the Dedicated Cloud Colocation Service to reduce risks of data compromise during shipment to and from the Data Center.

If Client provides its Equipment to NTT DATA in a condition such that NTT DATA is unable, as a technical matter, to provide the Colo Service, NTT DATA will return the Equipment to the Client-specified shipping address.

Service Offer

Colo Facilities and Equipment Services consist of the following:

- NTT DATA will provide the facilities and Colo Services in the applicable Data Center
- The Data Center facility is air-conditioned with secure raised floor space
- NTT DATA will coordinate with Client for management of installation and maintenance of Client's Equipment

Service Details
One-time Installation Services • Electrical power installation includes the preparation and connection of electrical power to NTT DATA provided cabinet Power Distribution Units (PDUs) or self-standing gear PDUs. This service also provides electrical receptacles and all electrical power wiring needed to connect the Equipment to the Cabinet's PDUs. Charges are incurred on a per power connection basis. • Network cable installation includes the preparation and installation of CAT6 network cabling from the Client provided network switches to the Client Equipment. This service also includes patch panel ports and all patch cables required for installation. Charges are incurred on a per cable basis. • Fibre cable installation includes the preparation and installation of fiber cable from a Client provided fiber switch to Client equipment. Charges are incurred on a per cable basis. • Equipment installation includes the preparation and installation of the devices into a designated cabinet. Charges are incurred on a per device basis.
Recurring charges • 48-unit cabinets contain 2 smart PDUs and top of the rack patch panels. Cabinets are sold in full cabinets increments. • Square Foot floor space for self-standing gear. Sold in square foot increments. • Electrical power in kilowatts. Sold per consumed kilowatt. • Smart Hands Support for physical touches/assistance in a month by NTT DATA personnel on Client's equipment. Sold per hour increments.

Client Responsibilities

The following Client responsibilities apply to all Dedicated Cloud Colo Services.

- Prior to purchasing the Colo Service Client must have purchased Dedicated Cloud services from NTT DATA.

- Client will configure the Equipment to be installed into the Data Center and will configure the Equipment for particular applications.
- Client will load the Client application and databases on the Equipment and ship the Equipment to NTT DATA using the address and shipping information provided.
- Client is responsible for shipping the Equipment from NTT DATA datacenter at Client's cost. A pre-paid return shipping label must be included and provided by the Client.
- Client will encrypt its data on the Equipment before shipping to NTT DATA.
- Client is responsible for the network routing of its server into its Dedicated Cloud environment once installation is complete.
- Client represents and warrants that it has obtained permission for both Client and NTT DATA to access and use, whether remotely or in-person, Client-owned or licensed software, hardware, systems, the data located thereon and all hardware and software components included therein, for the purpose of providing the Colo Service. If Client does not already have that permission, it is Client's responsibility to obtain it, at Client's expense, before Client asks NTT DATA to perform the Colo Service.
- Client will complete and retain a backup of all existing data, software and programs on all affected systems or Equipment prior to and during the delivery of this Colo Service. Client will make regular backup copies of the data stored on all affected systems or Equipment as a precaution against possible failures, alterations, or loss of data.
- Client is responsible for the restoration or reinstallation of any programs or data.
- The provision of the Colo Service 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. Client will ensure that NTT DATA's performance of the Colo Service will not affect such warranties or, if it does, that the effect will be acceptable to Client. NTT DATA does not take responsibility for third-party warranties or for any effect that the Colo Service may have on those warranties.

De-Installation and Return of Equipment (Optional Service)

De-installation is not included in and is out of scope of the Colo Service. Return shipment of Client Equipment is at the expense and risk of Client. NTT DATA is not liable for any data loss as a result of the de-installation or shipping process.

Insurance

Client will insure and keep insured Equipment against all manner of loss in an amount not less than replacement cost.

Exclusions

Following activities are excluded from the scope of the Dedicated Cloud Colocation Services:

- Design of Client's public cloud solution or environment
- Data design
- Synchronization of the Client's application and database with Client's Dedicated Cloud environment
- Application profiling, which includes identification of applications compatible with virtualization and analysis of server/application interdependencies
- Migration, loading or importation of Client Equipment-based data
- De-installation of Equipment
- Special projects for any physical adds/moves/changes or deletes or custom reporting

Appendix G: Cloud Backup service

Scope

Cloud Backup service is an optional add-on service to NTT DATA Dedicated Cloud that may be purchased under a separately agreed service description or statement of work. Subject to the terms provided in such separate agreement, the primary goals of Cloud Backup Service are to:

- Provide protection and recovery from accidental deletion or corruption of data;
- Provide protection and recovery from a complete server, Virtual Machine and / or infrastructure failure causing downtime or a loss of service;
- Provide application consistent data backup with granular recoverability for supported applications / databases;
- Provide options for redundant / offsite data copies;
- Provide options for the long--term retention of data;

Cloud Backup Services offers two service coverage levels, one of which the Client may select on the Order Form:

- Self-service
- Fully-managed

Additionally, the Client can subscribe to the appropriate service plans (which define schedules, number of data copies & locations, retention and recovery times) relevant to their business requirements.

Use Cases

Cloud Backup Services consist of three classes of offerings:

- Virtual server (hypervisor)
- File system
- Application / database

Virtual Server

The virtual server offering is provided to address the basic backup and recovery use cases for Virtual Machines, and consists of the following capabilities:

- Aimed at small to medium sized virtualized workloads.
- (e.g. 30GB – 300GB such as web servers)
- Agentless protection methods
- (Proxy based – hypervisor integrated)
- The ability to protect and recover:
    - Virtual Machine image
    - Virtual Machine disks and volumes

- In-place recovery or out-of-place recovery

File System

The File System offering is provided to service the granular backup and recovery use cases for Virtual Machines, and consists of the following capabilities:

- Aimed at workloads of any size
- (e.g. Web servers, management servers and file servers)
- Agent-based protection methods
- The ability to protect and recover:
  - Files & folders (including open file support)
  - Operating system
  - Individual file & folder recovery
  - Individual file download
  - Full system recovery (including recovery to disparate infrastructure)

Application / Database

- The Application offering is provided to service the advanced backup and recovery use cases for applications running in Virtual Machines, and consists of the following capabilities:
- Aimed at application / database workloads of any size
- Agent-based protection methods
- The ability to protect and recover:
  - Applications
  - Databases
  - Log Files
  - Full (point in time) application integrated recovery
  - Full (point in time) database integrated recovery
  - Granular application recovery (for supported applications)

Service

Service Plans

Cloud Backup Services consists of two service plans, one of which the Client may select on the Order Form:

- Basic
  Agentless backup for Virtual Machines images
- Advanced
  Agent-based backup for applications, databases or file systems

*Following are supported standard applications:

- Microsoft Exchange

Supported Matrix	Basic	Advanced
Service Features		
Compression	Included	Included
Deduplication	Included	Included
Data Encryption	Included	Included
Service Reporting	Included	Included
Alerts & Notifications	Included	Included
VM Auto-Discovery	Included	Included
Hypervisor / Virtual Machine Image Protection	Included	Included
File System Protection	Not included	Included
Application Consistent Protection	Not included	Included
Application Integrated Protection	Not included	Included
Database Protection	Not included	Included
Self Service Restore	Included	Included
File Download	Included	Included
File / Folder Restore	Not included	Included
Virtual Machine Disk / Volume Restore	Included	Included
Virtual Machine Restore	Included	Included
Application Restore	Not included	Included
Database Restore	Not included	Included
In Place Restore	Included	Included
Out of Place Restore	Included	Included
Offsite Copy / Replica	Included	Included
Service Options		
Standard applications*	Not included	Included
Other applications	Not included	Optional
Long Term Retention	Optional	Optional
Custom Schedule/Retention	Optional	Optional

- Microsoft SharePoint
- Microsoft SQL Server
- Oracle database

Below table provides parameters supported by the service plans.

Service Plans	RPO	Retention	Copies / Replicas
Basic	24hr	15 - 30 days	0 - 1
Advanced	15 min - 24hr	15 - 30 days	0 - 1

Note, additional charges shall apply in case the Daily Change Rate (amount of new or changed data per day on applicable Virtual Machine or Application) for instances that are included in the Services exceeds 10% under Basic Service Plan and 15% under Advanced Service Plan. For example, any files that were updated shall be considered a change. The Daily Change Rate formula is determined by NTT DATA and subject to change.

Roles and Responsibilities

The scope of NTT DATA Services responsibilities will depend on the chosen service coverage level. The below matrix identifies activities managed by NTT DATA Services.

Activity	Self-Service	Fully Managed
Portal for Client self-service operation of backup jobs and schedules.	Included	Included
Reporting Portal for on-demand self-service report generation of job success, failure and vault capacity.	Included	Included
FTP Site containing supported agents, configuration guides and help documents.	Included	Included
Service desk providing a single point of contact for Incident Management	Included	Included
Monthly Client usage billing report.	Included	Included
Management of backup infrastructure	Included	Included
Create and maintain default Service Plans (frequency, retention, storage, etc.)	Included	Included
Create and maintain custom Service Plans (frequency, retention, storage, etc.)	Optional	Optional
Register client / application and install agent	Not included	Included
Create and manage backup rules	Not included	Included
Configure Backup Failure Notification	Not included	Included
Re-start or re-schedule failing backup jobs up to three times in one day	Not included	Included
Escalation of persistent failing backup jobs to nominated Client contact	Not included	Included
Assisted support to determine and remedy issues with persistently failing jobs	Not included	Included
Automated daily and monthly email reports on backup job success and failures	Not included	Included
Receive restore request and execute	Optional	Optional

Appendix H: Disaster Recovery (DR) Service

Introduction to Cloud Disaster Recovery Service

The Disaster Recovery Service (the "DR Service") is an optional add-on service to NTT DATA Dedicated Cloud. The DR Service is a Client-managed disaster recovery service which provides a disaster recovery technology integrated to the Client's virtual environment.

Service Offer

Disaster Recovery Service Overview

The DR Service utilizes VMware's Site Recovery Manager (SRM) technology along with vSphere Replication or Array based to replicate the Client's VM environment to an alternate site based on a Client-defined disaster recovery plan.

The DR Service supports the scenario when both production and DR/Failover sites reside at the Dedicated Cloud. The scenario when production or DR/Failover site reside at Client site is supported for an additional charge.

NTT DATA will use Recovery Point Objective (RPO) and Data Change Rate information from the Client to design and implement the necessary infrastructure (including bandwidth) to support the following RPO targets: 30 minutes, 1-hour, 2-hour, 4-hour, and 8-hour. Please note that DR Service is a Client managed self-service offer. Therefore, the Client maintains control and responsibility for defining, implementing and the maintaining recovery plan along with RTO targets unless the services are contracted as an optional add-on service to NTT DATA under a separately agreed service description or statement of work.

The DR Service supports automated failover in the event of a disaster at the production site and provides failback once the source location has returned to normal. It also provides self-service failover testing capability that does not impact Client's production environment.

Infrastructure supporting the DR Services is subject to same SLA criteria set forth in Appendix A above.

Parameters of DR Service:

- Only one SRM per vCenter is allowed
- SRM does not provide protection for Active Directory domain controllers
- Array based replication limitations:
    - Array based replication has limit of up to 5000 VMS and only supports protecting a VM if all disks for the VM belong to the same array frame.
    - Non array-based replication has limit of up to 2000 VMS.
    - A VM that has multiple disks from different arrays is not permitted.
- Additional information on File Level Restore limitation can be found at: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2053871

The DR Service includes the following:

Services	Included
Replication & Recovery Technology	X
Cloud infrastructure for DR solution	X
Network bandwidth based on Client's RPO requirements and data change rate	X
Base installation & configuration of VMware SRM & vSphere Replication	X
Alerting and response to failed automated testing	X
DR Consulting Services - Recovery Plan Development	Optional

During the initial setup of the DR environment in the NTT DATA datacenter, NTT DATA will perform the following activities:

- Design and architecture layout documentation
- Installation & configuration of SRM servers and vSphere Replication in the Dedicated Cloud environment
- Provision & configuration of ESXi hosts, storage and vSphere Suite
- Initial seeding of Client data (via shipping of data on hard drive from Client to NTT DATA)
- Network connectivity – implement and test network connectivity
- Determine the bandwidth needed for SRM
- Knowledge transfer - operational training up to 10 hours on how to use the VMware SRM technologies delivered remotely
- Proof of concept test using NTT DATA's "Hello World" DR template

Post implementation Assistance

Any post implementation DR project-based work covering assistance such as re-architecting or testing assistance may be subject to additional charges based on engineering hours required for the requested work.

Out of Scope of DR Services:

- Management of VM operating systems
- Support of applications on the VMs
- Scripting support for automatic application launch/sequencing after a fail-over
- Installation and configuration of SRM at any site outside the Dedicated Cloud unless the services are contracted as add-on service to NTT DATA

Appendix I : Cloud Management Platform Service

Scope

The Cloud Management Platform ("CMP") is an included service within NTT DATA Dedicated Cloud. The CMP is designed to shorten the time required to provision and maintain infrastructure, which may be from days to minutes, through automation of IT service delivery and enables efficient management of private, public and hybrid clouds. CMP consists of an intuitive portal empowering user to perform a variety of self-service action for IT services across public and private clouds. CMP automates orchestration of middleware components, provisioning, OS layer configuration and integration with 3rd party products such as DevOps toolchain (Chef, Puppet, Ansible) and infrastructure-as-code. CMP enables governance of access, approval policies, and optimization features across public and private clouds. NTT DATA also enables representational state transfer (REST) application programming interface (API) access to the CMP which can enable a similar experience as the UI does from another system.

Definition of Terms

These terms are used within this document.

CMP	Current version of the Cloud Management Platform
AD	Active Directory used to support access to Client VM resources
CMP tenant user	User accessing the services via the Cloud Management Platform (CMP) Service Portal
Blueprint	Cloud Management Platform (CMP) Blueprint is a cloud-agnostic template for publishing a catalog item that a cloud user can use to request an infrastructure or application stack.
Catalog Item	vice Cloud Management Platform (CMP) Catalog Item is a blueprint.
Workflow	Cloud Management Platform (CMP) Workflow is for automating multi-step processes across the platform.
Orchestration	Cloud Management Platform (CMP) Orchestration extends the workflow engine to manage processes and to automate things outside of the CMP.

Pre-requisites

Some setup is required to be done in order to provide the Client access to the CMP. The Client's primary and secondary Active Directory (AD) server information needs to be obtained and network access defined. This allows network access for the CMP to authenticate the Client users in their CMP organization with their AD servers.

Service

The Cloud Management Platform Service includes a base package with several optional add-on services. The base package includes a tenant in a secure multi-Client CMP environment managed by NTT DATA with access to base workflows and blueprints (determined by NTT DATA). Additionally, Clients with more than 300 VMs onboarded in CMP are provided thirty (30) hours of remote consulting to provide a Service that conforms to individual Client requirements.

Additional development efforts must be scoped and purchased separately. NTT DATA will only provide support for the Client organization structure, discovery of existing cloud resources, manager/user roles defined, and NTT DATA covered Blueprints, Catalog Items and Workflows. The base package requires that NTT DATA has administrator access to hypervisor management software and the Client no longer having access to hypervisor management software. All Client VM actions are accomplished via the CMP Service Portal.

Add-on services are available for Clients who require NTT DATA to manage non-Dedicated Cloud environments and for Clients who require additional consulting services beyond what is included within the base package.

The following section provides a combined view on the solution features.

	Base Package
1. Initial Client configuration (including up to 2 hours of transition training)	Included
2. Development of Blueprints, Catalog Items and Workflows - (up to 30 hours) for Clients with more than 300 VMs onboarded in CMP	Up to 30 hours included
3. Leveraging NTT DATA knowledge repository to accelerate Client specific development	Included
4. CMP licenses	Included
5. Break fix support	Included
6. Upgrading and patching of CMP	Included
7. Service Requests (SRs)	Included
8. Incident Acknowledgement Time and Incident Resolution Time SLAs	Included
9. Ability to manage non-Dedicated Cloud environments	Optional
10. Cloud Management Platform consulting	Optional

1. Initial CMP Client configuration

Base package is limited to one (1) tenant organization in a secure multi-Client CMP environment. Multi-Client CMP environment is outside of the Client's environment.

The initial CMP onboarding service includes:

- Requirements gathering
- Establishing tenant organization within CMP
- Establish access from CMP to Client AD

- Base configuration consists of discovering existing VMs and apply appropriate attributes for each VM
- CMP Users Portal Guide
- Transition training delivered remotely, lasting up to two (2) hours maximum.

Initial Client service configuration does not include bespoke development of Client Blueprints, Catalog Items, or Workflows.

2. Development of Blueprints, Catalog Items and Workflows

Clients that onboarded more than 300 VMs in CMP get access to a maximum of (30) hours of Cloud Management Platform consulting services to assist the Client in creating and configuring Blueprints, Catalog Items, and Workflows. The consulting services are delivered following initial configuration as one project and may not be split between multiple projects. Extended Cloud Management Platform consulting services are available for purchase, if required.

Below is a sample project:

1. Requirements gathering
2. Development using NTT DATA's knowledge repository
    - 3 Workflows – 6 hours
3. Net new development
    - 2 Blueprints with Catalog Items – 12 hours
    - 1 Workflow – 8 hours
4. End-to-end testing – 4 hours
5. Client sign-off and acceptance

3. Leveraging NTT DATA's knowledge repository to accelerate Client specific development

The NTT DATA knowledge repository includes pre-created Blueprints and Workflows for most common scenarios. NTT DATA will leverage its knowledge repository to accelerate development of Client specific Blueprints and Workflows. This reflects in reduction of total development hours that NTT DATA will quote for such projects as applicable. The NTT DATA knowledge repository is for internal NTT DATA use only.

4. License Requirements

The CMP license costs are included within the CMP services agreement.

5. Break-fix support

NTT DATA will provide break-fix support to Client CMP environment. Break-fix support is limited to:

- Base Client organization configuration.
- Blueprints and Catalog Items developed by NTT DATA and included as part of CMP contract.
- Workflows developed by NTT DATA and included as part of the Services contract. Sub workflows are counted as individual Workflows.

6. Upgrading and Patching

NTT DATA will maintain the CMP patch and update compliance through an internal control process as a part of the service. All patching and update maintenance will be scheduled and executed following existing Dedicated Cloud change management standards. NTT DATA will determine the approved patch and update schedule to be applied to the CMP environments using best practices.

7. Standard Service Requests (SR)

Standard Service Requests are limited to the existing Service Request types within NTT DATA's ITSM tools, as applicable: BMC Remedy (OPAS) v2, BMC Remedy (OPAS) v3, and ServiceNow. Standard SRs are supported that are not due to disruption of service as determined by NTT DATA. SRs are limited to sixty (60) minutes in length. SRs will be assigned Severity Level 4 Priority and are subject to the Incident Acknowledgement Time and Incident Resolution Time SLAs as defined in Appendix A.

8. Incident Acknowledgement Time and Incident Resolution Time SLAs

Incident Acknowledgement Time and Incident Resolution Time SLAs are provided as defined in Appendix A.

9. Ability to Manage non-Dedicated Cloud Environments

CMP can support non-Dedicated Cloud environments through built-in functionality. Please contact NTT DATA for the full list of supported environments.

10. Cloud Management Platform Consulting

Additional consulting services may be used to address requirements that are out of scope for Service Requests and out of scope for break fix, such as:

- Blueprint development and customizations
- Catalog Items development and customizations
- Workflow development and customizations
- Orchestration development and customizations

Cloud Management Platform consulting services are offered on time and material (T&M) basis and delivered as individualized projects with bespoke timelines defined by NTT DATA once requirements gathering is completed.

Appendix J: Dedicated Cloud Encryption Protection

Introduction to Dedicated Cloud Encryption Protection

Encryption Protection service is an optional add-on service to NTT DATA Dedicated Cloud. The Encryption Protection solution protects data using strong encryption, privileged user access control and the collection of security intelligence logs.

The Encryption Protection solution is comprised of key management server and encryption agents.

The key management server is available in the following form: virtual server, standard physical appliance & FIPS 140-2 Level 3 compliant physical appliance. The key management server centrally manages keys and policies for all virtual machines that are configured for encryption protection. An encryption agent is installed in each virtual machine that requires encryption protection and the agent encrypts / decrypts data files as well as applications per Client's data encryption policy.

Encryption protection can be used to meet compliance requirements such as PCI DSS, HIPAA/HITECH, and to provide an extra layer of security for protected information of all kinds including backup media. Data encryption provides separation of duties between data security administrators and system administrators, allowing companies to secure protected information from being accessed by regular users and system administrators without restricting their ability to use and support the technology hosting the data.

The solution consists of two types of encryption agents:

- Transparent Encryption Agent: Allows the user to encrypt and decrypt data of any file type (pdfs, spreadsheets, scripts, images etc.) using policies created and stored in the key management server.
- Application Encryption Agent: Allows the user to encrypt and decrypt applications such as databases, big data and PaaS applications that require field level encryption, using policies created and stored in the key management server.

The Encryption Protection solution supports the following:

- Platform:-
    - Microsoft Windows Server 2003, 2008, 2012;
    - Linux RHEL, SuSE and Ubuntu;
    - Unix: IBM AIX HP-UX and Solaris
- Database:-
    - Oracle, DB2, SQL Server, MySQL

NTT DATA Responsibilities

Encryption Protection is primarily a Client self-service solution. NTT DATA is responsible for providing the infrastructure needed to run the solution, along with service desk support. The Client is responsible for access policy creation, configuration, and administration of the encryption protection solution.

- **Installation & Configuration**: – As part of onboarding the Client to the Dedicated Cloud service, NTT DATA will provision and configure a VM (assign network IP address) and install the key management solution on that VM.
- **Licensing**: – NTT DATA will perform initial configuration with a trial license and upon full onboarding of the Client on the Dedicated Cloud environment, NTT DATA will provide a permanent license file to the Client and the Client will need to update the key management server with the permanent license file.
- **Encryption protection Solution (software) Update**: – NTT DATA will not undertake any activity to update the encryption protection solution meaning that NTT DATA (will not update the key management software, or the agent software). However, NTT DATA will notify the Client of available software updates. It will be up to the Client to decide when and which software (key management server, transparent agent, application agent) to update at the Client's cost.

Client Responsibilities

- **Set Access Policy**: Client must develop their own access policy and configure the key management server according those policies. Client should follow the User Guide provided during the Onboarding setup to install the agents and set up policies on the key management server.
- **Maintenance of Client Encryption Policy** – Clients are responsible for maintaining their encryption policies.
- **Audit & Reporting** – Clients are responsible for generating reports from the key management tool and performing required audit.

The following table summarizes NTT DATA's and Client's responsibilities:

Category	Activity	NTT DATA	Client
Client Onboarding	Provision VM for Key Management	X	
Client Onboarding	Create License file	X	
Client Onboarding	Initial Installation of the Key Management software	X	
Client Onboarding	Configure Firewall	X	
Client Onboarding	Configure Change Auditor for Key Management alerts	X	
Client Onboarding	Configure Key Management software		X
Level 1 Support	Answer to a Client question	X	
Level 1 Support	Suggestion of how to accomplish a particular task	X	
Level 1 Support	Workaround to a Software issue	X	
Level 1 Support	Open Level 2 or Level 3 ticket	X	
Level 2 Support	Software not operating as documented	X	
Level 2 Support	New feature or functionality requested	X	
Level 3 Support	Unresolved L2 support requests	X	

Access Policy	Create access policies		X
Access Policy	Maintain access policies		X
Administration	Add host names to Key Management database		X
Administration	Install agent software to hosts		X
Administration	Create, add, delete Key Management administrators		X
Administration	Reset passwords for all Key Management administrators		X
Administration	Addition and deletion of domains		X
Administration	Assign administrators to domains		X
Administration	Configure Key Management preferences and logs		X
Administration	Backup and restore the Key Management database		X
Administration	Configure high availability		X
Administration	Configure syslog servers for system-level messages		X
Administration	Installation of the license file		X
Administration	View and download system-level reports		X
Administration	Notify Client of Key Management software updates	X	
Administration	Update Key Management software		X
Administration	Add and remove Key Management administrators in domains		X
Administration	Configure syslog server for application-level messages		X
Administration	View and download domain-level reports		X
Administration	View Key Management preferences and logs		X
Administration	Create and configure signature sets		X
Administration	Configure keys and key groups		X
Administration	Configure online and offline policies		X
Administration	Configure protected hosts and host groups		X
Administration	Sharing a host with another domain		X
Administration	Export and import keys		X
Administration	View Key Management security administration preferences and logs		X

Appendix K: Utility Zone service (Utility Zone)

Scope of Utility Zone service

The Dedicated Cloud Utility Zone service is an optional add-on service to NTT DATA Dedicated Cloud. The Dedicated Cloud Utility Zone service enables additional capacity of the Dedicated Cloud core infrastructure (compute and storage) without multi-month commitment. The Utility Zone service, when enabled, deploys to the same data center and network as Client's existing Dedicated Cloud infrastructure. The Utility Zone Service is designed for non-persistent workloads and not recommended for persistent, storage-intensive workloads.

The Utility Zone service provides access to following infrastructure:

- Compute (compute hosts)
- Storage

Additional infrastructure is deployed as part of the Utility Zone service and follows the same service standards described in the Dedicated Cloud Service Description subject to certain limitations as described below. The Utility Zone service is enabled to include access to the existing Client Dedicated Cloud network and within the same datacenter as the current Dedicated Cloud service. The amount of additional infrastructure a Client may gain access to via the Utility Zone service is limited by a predefined Storage Cap and Compute Cap. The Compute Cap is calculated using the formula as described in the Compute section below and is variable based on the size of the Client's current environment. The Storage Cap is calculated based on the formula as described in the Storage section below and is based on the number of compute hosts in Client's Utility Zone.

Pre-requisites

- Prior purchase of NTT DATA Dedicated Cloud Service.
- Client is required to enable the Cloud Management Platform Service (Appendix I) in order to use Utility Zone service. The Cloud Management Platform is used to manage the Utility Zone infrastructure through a self-service interface.
- VMware based Reference Architecture.

4.1. Compute

The Utility Zone service provides access to compute hosts that are similar in configuration to those listed in this Service Description, subject to availability. A minimum of two (2) compute hosts are required to be deployed as part of the Utility Zone service to ensure continued high-availability.

NTT DATA has established a Compute Cap for each Client environment. This cap is defined as maximum number of compute hosts that a Client can deploy as part of their Utility Zone infrastructure. The Compute Cap is set at two (2) for Clients with Dedicated Cloud environments smaller than forty (40) compute hosts. For Clients with greater than forty (40) compute hosts, the Compute Cap is calculated as five percent (5%) of total number of compute hosts in their Dedicated Cloud environment. Provisioning of additional compute hosts above the Compute Cap requires NTT DATA approval and is addressed on case-by-case basis. NTT DATA reserves the right to change the

Compute Cap with notice to Client. NTT DATA will use commercially reasonable storage capacity to maintain sufficient Compute capacity to meet Client needs up to the Compute Cap, but during periods of very high demand it is possible that delays may be necessary prior to provisioning additional Utility Zone compute hosts.

NTT DATA requests that Clients provide a planned end of service date (non-binding) at the time of deployment. Clients may change the planned end of service date for compute hosts at any time.

4.2. Storage

The Utility Zone service enables additional access to Standard Tiered Block Storage as described in the service details and options section of Dedicated Cloud Service Description. Storage will be billed in storage clusters that are made available to the Utility Zone. Virtual Machines deployed in the Utility Zone can only be LUN masked with storage clusters deployed in the Utility Zone and vice versa.

NTT DATA has defined a maximum amount of storage per compute host that Client can deploy as part of Utility Zone infrastructure. This Storage Cap is set at two (2) terabytes (TB) per deployed compute host. Provisioning of additional storage above Storage Cap requires NTT DATA approval and is addressed on case-by-case basis. In the event the Storage Cap is exceeded through Client reduction of the number of compute hosts deployed, NTT DATA reserves the right to decrease amount of storage in Client's Utility Zone with notice to Client. NTT DATA also reserves the right to change Storage Cap. NTT DATA will use commercially reasonable efforts to maintain sufficient storage capacity to meet individual Client needs, however, during periods of very high demand it is possible that delays may be necessary prior to provisioning additional storage in the Utility Zone.

The Utility Zone service allows Client to add storage at any time. Storage decreases will be accommodated separately, only once per month. NTT DATA will establish and communicate the time and date window within the month prior to commencing the Utility Zone service. Storage clusters may be added and removed in increments of two (2) TB volumes only.

4.3. Networking

The provisioned Utility Zone Infrastructure has access to same networking resources that are available within the Client's existing Dedicated Cloud environment.

4.4. Cloud Management Platform

NTT DATA will build and maintain Blueprints, Catalog Items and Workflows required to support Utility Zone service. Refer to "Appendix I" topic "Cloud Management Platform Consulting"

4.5. Reporting

NTT DATA will provide following additional Utility Zone reports to Client via self-service or upon request:

Service Category	Report Title	Frequency	Comments
Utilization	Storage pools and volumes	Daily	Data on storage clusters, storage provisioned and used for Client VMs in Client's Utility Zone
Utilization	VM machine inventory	Daily	List of all Client cloud VMs with associated ESX host names, DNS names, container names in Client's Utility Zone
Utilization	Host inventory	Daily	Listing of all Client ESX hosts (if applicable) and VMs located on each host in Client's Utility Zone
Utilization	Billing	Monthly	List of Utility Zone usage during billing period including compute hosts, VMs and Storage with associated charges

SLAs

- Incident Acknowledgement Time and Incident Resolution Time SLAs apply as set forth in Appendix A.
- Availability SLAs do not apply to Utility Zone.

Pricing

The methodology for determining invoice amounts for the Utility Zone service provided under this Service Description is as follows:

Service Fees:

Services	Frequency	Unit
UZ, Blade Servers	Daily	per Blade
UZ, Virtual Machines	Daily	per VM
UZ, Compellent Standard Tier Storage (SAS / SSD)	Monthly	per GB

Pricing:

1. Utility Zone pricing does not include cost of maintaining Blueprints and Workflows that are required to provision and deprovision compute hosts, virtual machines and storage to the Utility Zone.
2. Utility Zone pricing does not include other costs of the Cloud Management Platform such as a per virtual machine fee.
3. NTT DATA will bill for delivered Utility Zone service on a monthly basis.

Client Obligations

Utility Zone specific Client obligations:

- Client will verify that infrastructure has been moved to Client environment successfully and will inform NTT DATA in case of any issues
- Client is responsible for capacity management in Utility Zone
- Client will initiate provisioning/de-provisioning of infrastructure if needed