NTT DATA Dedicated Cloud
Service Description

Version 5.0 | June, 27, 2017

NTT DATA Services
formerly Dell Services

Table of Contents

Service Description

NTT DATA Dedicated Cloud

Introduction

NTT DATA Dedicated Cloud ("Dedicated Cloud") is infrastructure as a service (IaaS) offering designed to provide a secure private cloud environment, hosted and managed by NTT DATA. Base service includes security, monitoring, support, and administration up to 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 additional charge.

The table below identifies infrastructure components that are dedicated to Customer and components of the Dedicated Cloud that are shared between Customer and NTT DATA's other customers.

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 Machnies

You can create, modify and decommission Virtual Machnies (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 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. Customer 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 operating system (OS) guest licenses can be purchased from NTT Data:

Microsoft Windows Server Operating System for each host	Optional
Red Hat Enterprise Linux	Optional

Networking

NTT DATA supplies unmetered local area network ("LAN") access to the Customer'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 Customer 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 Customer with an isolated network that can be deployed based on their unique requirements. NTT DATA provides Customers with individual virtual switches, firewalls, and virtual local area networks ("VLANs"), allowing us to meet the segregation/isolation needs of each Customer.

Dedicated Cloud offers following networking capabilities:

Public IP addresses	Optional
Internet – committed bandwidth Provides committed bandwidth that is reserved for the Customer's consumption (includes 4 Public IP addresses).	Optional
Internet – burstable bandwidth Bursting capabilities allow Customers to account for that extra level of bandwidth needed to accommodate peak demand. Burst bandwidth is not dedicated; rather burst bandwidth includes shared traffic. Accordingly, performance degradation may occur when Customer is utilizing Burst bandwidth. (see Appendix G for additional details)	Optional
VPN Managed Internet Protocol Security (IPSEC) VPN services providing site-to-site connectivity	Optional
Remote access VPN Customers can access their Dedicated Cloud environment remotely using secure and flexible SSL VPN	Optional
Software Defined Network Customer's software defined network with multiple isolated tiers (e.g. application, database, and web).	Optional
Software Defined Network – Managed firewall SDN based managed virtual firewall	Optional, available only if SDN is purchased
Software Defined Network – Load Balancer SDN based managed virtual load balancer	Optional, available only if SDN is purchased
Managed virtual firewall context A managed virtual firewall context to enable customer defined firewall security policies	Optional

Advanced Load Balancing (LB) Virtual load balancing suitable for internet facing or backend VM load balancing.	Optional

Storage

Dedicated Cloud offers following storage tiers:

Standard Tiered Block Storage Dedicated logical unit number (LUN) defined as mix of 10K RPM and SSD tiered storage. Default write occurs to 10K RPM drives and very active data gets auto tiered to SSD to provide higher server performance at a low price point.	Included
Performance Tiered Block Storage Dedicated LUN defined as mix of SSD and 10K RPM storage. Default write occurs to SSD and auto tiered down to 10K RPM drive for inactive data. This solution is ideal for databases and other I/O intensive applications.	Optional
Extreme Performance (SSD) Tiered Block Storage Read and write intensive SSD only storage provided as LUNs that is recommended for applications that need consistently very low latency. The data is written to write intensive SSD. Infrequently changed data (read only data) is auto tiered to read intensive SSD.	Optional
NFS Ability for the Customer to manage the storage directly at the VM level. Provided as LUNs, can be shared across VMs and clusters.	Optional
Daily snapshots of all storage arrays. **Applies to all storage tiers. Copies are maintained for a rolling 3 day period. Backup is at the LUN level (selection of individual files is not supported).** Note: Daily snapshot does not guarantee full recovery of data.	Included

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 Customer data from being modified during transmission.
- Confidentiality: Dedicated Cloud is designed to allow only authorized users (as nominated by the Customer) to access information in their virtual environment using logical isolation and segmentation techniques for leveraged core network and storage components. Customers receive dedicated compute nodes. There is no multi-tenancy of Customer 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 offers following Security and Compliance options:

Physical, Technical and Administrative controls (below hypervisor)	Included
Intrusion Detection Systems (IDS) Enterprise-grade intrusion detection systems (IDS) in place to inspect Dedicated Cloud infrastructure management networks as 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 N for additional details)	Optional
HIPAA and HITECH Dedicated Cloud offers optional HIPAA- & HITECH-compliant security and privacy controls that enable healthcare-sector Customers to host electronic protected health information (ePHI). Healthcares customers (i) see Appendix E which includes a HIPAA matrix that lists NTT DATA's responsibilities versus the Customer's responsibilities, and (ii) are subject to the Business Associate Agreement set forth in Appendix E.	Optional
PCI The Dedicated Cloud environment has been designed in accordance with the PCI DSS Level 1 Service Provider standard. (See Appendix F for additional details) PCI Customers see Appendix F 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 Customer's responsibility. In many cases, NTT DATA and the Customer will be responsible for the identified control, but, as indicated above, NTT DATA's responsibility ends at the hypervisor and Customer must manage these controls within the context of its virtual data center environment.	Optional, available in select Data Centers

Overview

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

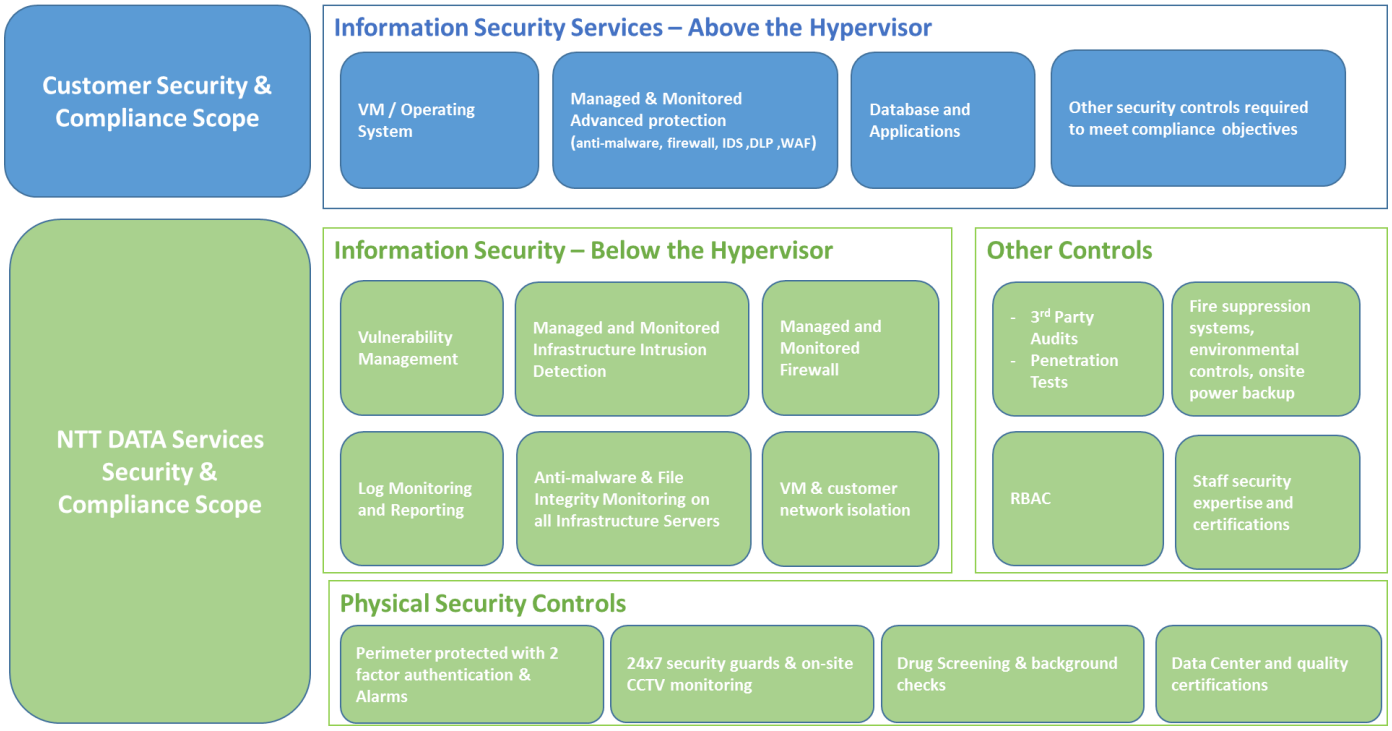
- **Physical controls**: Including environmental controls are countermeasures that affect the physical environment. Examples of physical controls include two-factor physical access controls, fire prevention systems, cooling systems, exit routes, security personnel and data center surveillance monitoring. 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; for example, firewalls, anti-malware, file integrity monitoring, intrusion detection systems, and encryption mechanisms.
- **Administrative controls**: Countermeasures that involve policy and procedures; for example, security and incident response policies, log audits, vulnerability scanning and penetration testing.

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

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

NTT DATA security and compliance responsibilities extend from the data center floor up to the hypervisor. The Customer is responsible for their own security and compliance controls and program above the hypervisor (unless these security services are contracted as add-on service to 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 Customer 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. Dedicated Cloud with the applicable Data Centers (formerly Dell Services) and supporting services are ISO/IEC 27001 certified: http://i.dell.com/sites/doccontent/corporate/corp-comm/en/Documents/dell-ISMS-ISO27001.pdf.

- 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 Customer information and to strictly control network access to the Data Center. Customers connect with Dedicated Cloud via IPsec, MPLS, and Dedicated Circuit connections to provide security and privacy of network transmissions, and to help prevent Customer 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: Customers 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 Customers 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 Customer 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 Customers.

- 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 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 Customer 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 – Customer Delivery Executive (CDE)	Optional

NTT DATA will designate a named Customer Delivery Executive ("CDE") to the Customer account to manage overall service delivery and continuous improvement activities.

The CDE will serve as the single point of accountability in delivering Dedicated Cloud, providing following support:

- Establish and manage relationship with identified Customer contacts
- Define key measures for Dedicated Cloud and periodically review them with Customer
- Pro-actively explain any high severity incidents, root causes, and resolution efforts for Dedicated Cloud
- Develop and review cloud plans with Customer including forecast and growth projections for Customer
- Answer Customer questions related to billing and invoices
- Point of contact for any Customer escalations

Cloud Management Platform Service

Cloud Management Platform	Optional

The Cloud Management Platform (CMP) is an optional service that shortens the time required to provision infrastructure from days to hours through automation of IT service delivery and enables efficient management of private, public and hybrid clouds. CMP consists of an intuitive portal empowering administrators and users to request and a manage variety of 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 IT Service Management (ITSM) tools. CMP enables governance of access across public and private clouds. See Appendix M for additional details.

Backup and Disaster Recovery

Dedicated Cloud offers following Backup and Disaster Recovery options:

Data Protection (backup) service – self service Provides image and file level backup and restore. This solution stores backup images in-house on a different storage array than the primary storage frame, Customers can set retention cycles based upon standards they already have in place (See Appendix L for additional details)	Optional
Disaster Recovery (DR) service – self service 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 K for additional details)	Optional

Other optional services

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 Customer's servers/devices and Customer'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 I for additional details)	Optional
Managed Cloud Services Available for those Customers that prefer to have NTT DATA manage their operating systems, databases, applications, back-up appliances. (See Appendix J for additional details)	Optional

Technical Support

You may use the Cloud Lifecycle Manager Portal or contact the Service Desk via phone 24x7x365 for technical support. Cloud Lifecycle Manager Portal can be accessed from https://nttddc.vistarait.com/login.do.

To reach the Service Desk, dial the toll-free number +1 855-350-4372 with intelligent voice response (IVR). Additionally, Customers may email the Service Desk at Managed_Cloud_Services@Dell.com. Customer may assign up to 5 named contacts to contact the Service Desk on behalf of the Customer.

The Service Desk is a central point of contact for handling Customer issues. Service Desk functions include:

- Logging and routing the Customer raised incidents to the cloud engineering or account assigned Customer Delivery Executive (CDE)
- Providing assistance in raising service requests using Cloud Lifecycle Manager Portal
- Respond to inquiries around existing incidents or any service disruption statuses
- Routing billing inquires to billing department and to Customer Delivery Executive

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

Customer Self-Service Password Reset

Customer will access the Quest Password Manager (QPM) self-service portal site located at https://qpmext.dellcloud.com to unlock/reset their domain account password used to authenticate and access the Cloud Management Platform.

Customer will be using NTT DATA Active Directory user name and password credentials to get authenticated in the QPM interface and Cloud Management Platform. Whenever Customer requests to change password/unlock their accounts via QPM, their request will immediately update the NTT DATA Active Directory database. Customer receives their NTT DATA supplied NTT DATA Active Directory account at the beginning of their engagement.

The QPM password reset is not applicable where Customer chooses other authentication methods to access Cloud Management Platform such as extending their NTT DATA Active Directory to be integrated with their NTT DATA hosted Dedicated Cloud environment. In such cases, Customer is responsible for supporting any password reset operations using their own internal available methods and this is not within the scope of Dedicated Cloud.

If the Customer's end user has to reset their password using the QPM, another reset is not allowed for 24 hours. All passwords must meet the Dedicated Cloud password complexity policy. QPM stores the previous 10 passwords. In the event the Dedicated Cloud experiences any downtime Customer may not be able to reset their password until Dedicated Cloud becomes available.

Customer may contact NTT DATA Service Desk, if they forget their profile password and request the NTT DATA Service Desk to create an incident/task to reset the password.

Roles and Responsibilities Matrix

The following metrics and legends are used to define NTT DATA and Customer 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	Customer
Support service enablement Onboarding activities		P
Provide timely access to Customer resources if needed, including but not limited to, virtualization administrators and engineering, and project management.		P
Providing, installing and configuring the Dedicated Cloud Infrastructure (including hypervisor and hardware).	P	
Providing VMware licensing for Dedicated Cloud.	P	
Monitoring the Dedicated Cloud Infrastructure.	P	

Supporting and troubleshooting the Dedicated Cloud Infrastructure.	P	
Scheduling and communicating through the standard ITIL change management process, Dedicated Cloud Infrastructure changes and maintenance.	P	
Upgrading and patching the Dedicated Cloud Infrastructure.	P	
Manage and maintain Data Cener(s), racks, power and cooling	P	
Adding Cloud Dedicated Infrastructure (based on change orders).	P	
Removing Dedicated Cloud Infrastructure (based on change orders).	P	
Providing monthly Dedicated Cloud Infrastructure capacity reports upon request.	P	
Capacity planning and forecasting for Customer assigned Dedicated Cloud Infrastructure.	H	P
Providing utilization and SLA reports upon request	P	
Managing Customer'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
Compute Specific Section		
Activity	NTT DATA	Customer
Customizing and hardening templates (if required).		P
Maintaining customized and hardened templates.		P
Providing licensing for all software and applications used for Dedicated Cloud othger than software provided by NTT DATA.		P
Virtual to virtual (V2V) conversions.		P
Notifying Customer when cluster compute resources reach 75% utilization.	P	
Maintaining cluster compute resources under 85% utilization, by approving additional capacity or removing workloads.		P
Modifying and tracking 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
Provisioning and deprovisioning virtual servers in Customer's virtual environment.		P
Network Specific Section		

Activity	NTT DATA	Customer
Defining network subnets and IP space for Customer's Dedicated Cloud environment.		P
Assigning and managing IPs inside subnets.		P
Creating network subnets and VLANs inside NTT DATA Dedicated Cloud Infrastructure upon request.	P	
Operating, maintaining, and troubleshooting all physical and virtual network components residing in the Customer's Dedicated Cloud Infrrastructure.	P	H
Providing NTT DATA managed firewall	P	
Defining firewall rules.		P
Creating and maintaining firewall rules.	P	
Defining load balancer rules.		P
Creating and maintaining load balancer rules.	P	
Creating and maintaining Dedicated Cloud internal routing.	P	
Providing managed VPN services for site-to-site connectivity over the internet (IPsec connections).	P	
Troubleshoot site-to-site VPN connections	P	P
Design and implementation of 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	Customer
Provisioning storage from Dedicated Cloud arrays to host(s).	P	
Performing daily snapshots of Cloud storage arrays and maintaining copies for a rolling 3-day period.	P	
Notifying Customer when storage datastores reach 75% utilization.	P	
Maintaining storage datastores under 85% utilization, by approving additional capacity or removing workloads.		P
Support backup/recovery requests from daily snapshot of Cloud Storage arrays, which may include additional costs to the Customer to be agreed in advance and be subject to a separate agreement	P	
Security and Compliance Specific Section		
Activity	NTT DATA	Customer

Monitoring the system logs up to the hypervisor level.	P	
Monitoring IDS events up to the hypervisor level.	P	
Performing internal and external vulnerability scans on the Dedicated Cloud Infrastructure up to the hypervisor on a quarterly recurring basis.	P	
Performing external and internal penetration tests annually on the Dedicated Cloud Infrastructure up to the hypervisor.	P	
Audit annually to the SSAE 16 Type 2 standard	P	
Maintain ISO / IEC 27001:2005 certification	P	
Providing security management and access controls for in-service Virtual Servers and it associated vLANsincluding Customer software and data.		P

Exclusions

For the avoidance of doubt, the following activities are not included in the scope of this 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 Customer.
- NTT DATA will not be responsible for defects or malfunctions in third party software running in VMs encountered during the process of troubleshooting, resolving, patching, upgrading or maintenance.
- This Service Description does not confer on Customer any warranties which are in addition to the warranties provided under the terms of your master services agreement or Agreement, as applicable.
- If Customer does not implement NTT DATA recommendations for reducing alert and incident noise, service level commitments on those devices will not apply.

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 blade) added within the last 7 days of the month will not be charged for the month in which the capacity is added. Customer will be charged the full amount starting the next month. Capacity additions added prior to the last 7 days of the month will be charged the full, non-prorated rate for the month in which the capacity was added.

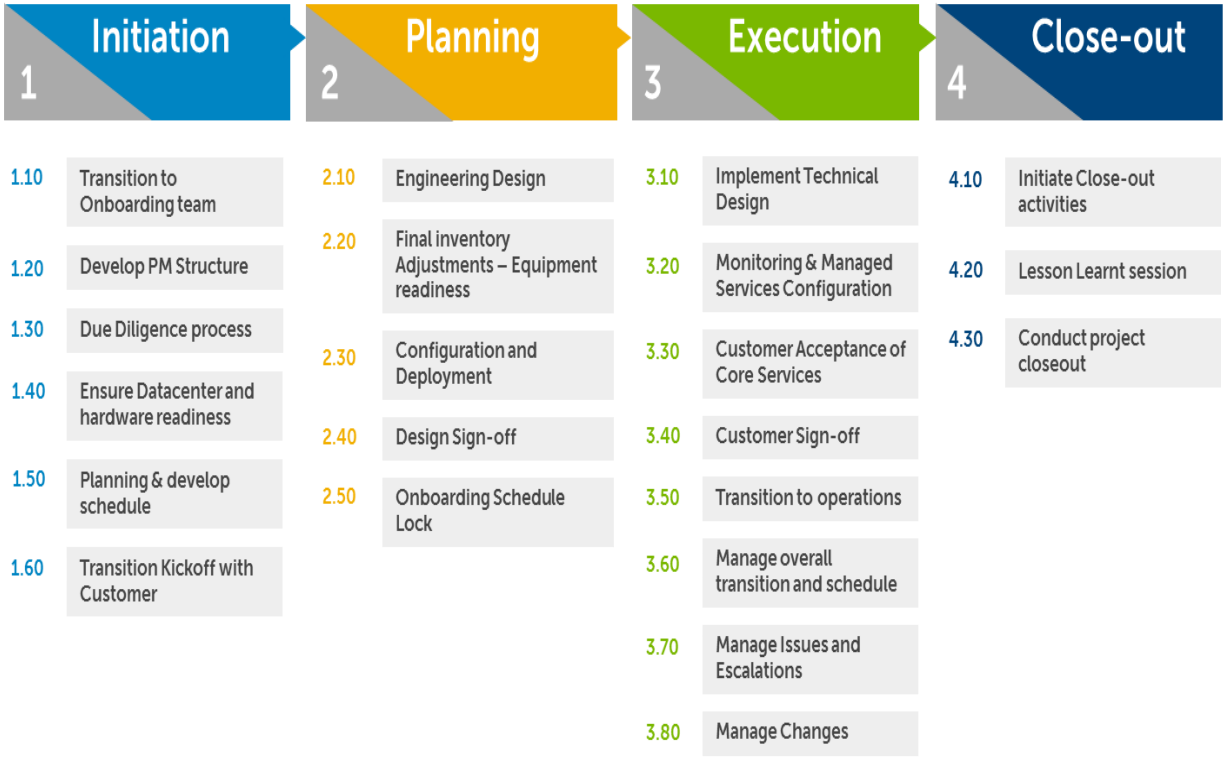
Dedicated Cloud is offered with a minimum one (1) year contract. At the end of the contract, Dedicated Cloud will automatically be renewed for another year unless sufficient written notice (30 days) is provided by the Customer to the contrary to your NTT DATA account representative.

For billing-related questions, please email DL-CDE-NTTDDC@Dell.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. Customer will be billed by NTT DATA, or will pay the service provider directly, for shipping of its Equipment to the datacenter.

Onboarding Process



The NTT DATA's onboarding team will collaborate with a designated Customer point of contacts to provide standardized onboarding of Dedicated Cloud. A high-level overview of the Onboarding process is set forth above. Following the Activation Date an assigned NTT DATA Project Manager will contact Customer to initiate Onboarding the project. The NTT DATA Onboarding Project Manager and Customer designated resource will serve as the point-of-contact for all communications, escalation of issues and any modification to the services procured in the order during the onboarding project.

Customer's onboarding responsibilities:

- Provide environment requirements
- Validation of configuration data and system integrations as applicable
- Provide escalation and notification contacts
- Provide Sign-off to NTT Data to confirm acceptance within 5 business days

NTT DATA's Project Management Responsibilities

- Manage NTT DATA tasks, resources associated with Dedicated Cloud, and coordinate activities with Customer.
- Conduct meetings to communicate roles, responsibilities, review assumptions, and schedule activities.
- Use standard industry recognized project management tools and methodologies.
- Employ a reporting mechanism to identify project tasks, next steps, and issues.
- Receive Customer sign-off at the completion of Onboarding tasks and hand over to steady state support.

At the conclusion of the onboarding project, deliverables will include;

- Customer's connectivity to core infrastructure (compute, storage) through agreed networking solution.
- If purchased credentials and access to Cloud Management Platform for holistic management of your environment.
- Customer "getting started" guide that will provide information necessary to operate the environment and include key contacts.
- Training and access to Cloud Life cycle Manager Portal to facilitate on-line request and incident management.
- Enablement of optional services on top of the base private cloud services.

Requesting Changes to Dedicated Cloud

Customers may add/change their services selection picking from standard service catalog options or custom service capabilities. There are two methods to request and additional change to an existing service:

- Leverage Cloud Lifecycle Manager Portal (https://nttddc.vistarait.com) to request changes or additions to Dedicated Cloud using a standard service catalog (if enabled)
- Alternatively leverage the Change Order process mentioned in the Order Form to request changes or additions to Dedicated Cloud

An Order Form signed by the Customer or submitted by the Customer as a self-service request through Cloud Lifecycle Manager Portal is required to start implementing changes or additions to Dedicated Cloud.

Changes and Addition:

- Standard Service item additions/change will be handled in 5 business days of the date of submission of a signed NTT DATA Change Order form or request ticket subject to availability of physical resources at the time of request. This timeline will apply to changes or additions to storage, blade, Microsoft license, committed bandwidth, vLAN, VPN, firewall, as well as modifications to existing data protection, modifications of existing Disaster Recovery, replication (WAVE) 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 mutually agreed schedule between NTT DATA and the Customer.
- Reductions in storage will be subject to Customer freeing up the storage space before the storage decommissioning can commence.
- Reducing dedicated blade count or storage (in excess of 100Tb) from Service subscription are subject to the terms agreed on the NTT DATA Order Form and will require payment of subscription fees for the remainder of the term.

Miscellaneous

1. The following will apply if Customer 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 Customer 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 responsibilities for making such determination remain and reside with Customer and any risk for any failures of Customer to adhere to applicable privacy and data protection laws by transferring or disclosing data to NTT DATA hereunder will remain exclusively with Customer. Customer will be responsible for obtaining any third party rights, permissions and consents or providing any notices to third parties as may be required in respect of the above. Customer represents and warrants that it has obtained all rights, permissions, and consents necessary for NTT DATA to obtain, access, process, host, transfer, or otherwise use, as applicable, any Customer 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 the Customer 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, Customer 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 Customer 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 availability or change without notice at any time. NTT DATA and its affiliates cannot be responsible for errors or omissions in typography or photography.

Terms & Conditions

This Service Description is governed by and subject to the terms and conditions in Customer's separate signed master services agreement with NTT DATA to the extent such agreement explicitly authorizes Customer 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.

Availability SLA

During the term of the applicable Order Form between NTT DATA and Customer 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 Customer 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 Customer's network, (iv) failures that result from changes to network circuits from Customer 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 Customer, (vii) failures attributable to the acts or omissions of the Customer, a vendor or an entity to which Services are provided, (viii) Customer exceeds 85% of virtual server cluster capacity, (ix) total used storage exceeds 85% of purchased storage, or (x) failures that result from changes performed by Customer 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 Customer's virtual servers. For example, if Customer has 10 virtual servers, each of which is not expected to be available during a weekly four-hour maintenance window, the Scheduled Uptime for Dedicated Cloud for that particular week would be 98,400 minutes: [10 virtual servers * ((60 minutes * 24 hours * 7 days) – (60 minutes * 4 hours*4 weeks))]. If the actual Uptime for these 10 virtual servers during a month (in this case a month with 28 days) is 392,850, Availability for that month would be 99.8% (392,850 minutes divided by 393,600 minutes multiplied by 100).
"**Uptime**" means the total number of minutes within any whole month that the Customer's virtual servers are available for use by the Customer. For clarity, Uptime will not be reduced as a result of any Exceptions and Exclusions.

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

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

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

Performance SLAs

During the term of the applicable NTT DATA Order Form between NTT DATA and Customer 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 Customer's account with NTT DATA is current and not suspended, Customer 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 Customer 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 Customer-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 blade is down, part of the database cluster is inoperable).

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

"**Severity Level 4**" 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 Customer report is formatted incorrectly).

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

Incident Acknowledgement Time SLA

Objective	Measures the aggregate acknowledgment time for Severity Level 1, Severity Level 2, Severity Level 3 and Severity Level 4 incidents.
Method	
Data Capture	Incident records in the Service Management Workflow System are used to determine the total number of Severity Level 1, Severity Level 2, Severity 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. Customers 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, Customers 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 Customer or Customer's vendors. Service Requests are excluded from SLA calculations. Incidents determined to be within Customer's responsibility to resolve are excluded from the calculations. Incidents determined to be caused by Customer'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. Customers 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, Customers 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 Procures and Credit Limitations

Claim Procedure: To receive a Credit, Customer 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:

Customer'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 Customer contact; the date(s) and times for each claim of downtime if claiming an Availability Credit; and the Performance SLA that was not achieved if claiming a Performance Credit.

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

Appendix D: Reporting

NTT DATA will provide following reports to Customer, on request:

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

Appendix E: HIPAA and HITECH

Business Associate Agreement for NTT DATA Dedicated Cloud

This Business Associate Agreement ("BAA") applies to Dedicated Cloud when that service is purchased directly from NTT DATA. Any capitalized terms used in this BAA that are not defined herein shall have the meaning ascribed to them in Health Insurance Portability and Accountability Act of 1996 as contained in 45 CFR parts 160, 162 and 164 ("HIPAA") and Subtitle D (Privacy) of Title XIII of Division A and Section 4104(b) of Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (the "HITECH Act").

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

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

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

- **Information Safeguards**: When NTT DATA has possession of PHI, is accessing PHI, or is transmitting Electronic PHI ("ePHI"), it shall (a) use appropriate safeguards as required by the HIPAA Privacy Regulations to prevent the use or disclosure of PHI otherwise than as permitted or

required under this BAA; and (b) with respect to ePHI, implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of ePHI as required by, and as more specifically set forth in, the HIPAA Security Regulations. NTT DATA's obligations described above will include additional safeguards required to be taken by NTT DATA pursuant to Section 13401(a) of the HITECH Act. Notwithstanding the foregoing, when NTT DATA is present at a facility of Customer or its affiliates or is accessing or utilizing equipment, software, tools, network components or other information technology owned, leased or licensed by Customer or its affiliates ("Customer Systems"), NTT DATA will comply with Customer's standard safeguards to prevent the use or disclosure of PHI (including Customer's standard administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of ePHI) applicable to such Customer facility or such Customer System, provided Customer has given NTT DATA prior notice of such safeguards in writing or in the same manner as Customer provides notice of such safeguards to its own employees and other contractors. Except as otherwise described herein, NTT DATA is not responsible for implementing safeguards with respect to the facilities of Customer or its affiliates or Customer Systems. For purposes of clarity, Customer and NTT DATA's respective safeguard obligations are set forth in Table 3 below, "HIPAA Safeguard Responsibility Matrix."

- **Security Incidents and Breach of Unsecured PHI**: NTT DATA shall report to Customer (a) any use or disclosure of PHI by NTT DATA in violation of its obligations under this BAA of which it becomes aware; and (b) any Security Incident relating to ePHI of which it becomes aware. In addition, NTT DATA shall, following the discovery of a Breach of Unsecured PHI, notify Customer of such Breach in accordance with the HIPAA Breach Notification Rule set forth at 45 C.F.R. § 164.410 Subpart D. With respect to unsuccessful Security Incidents, NTT DATA represents that the significant number of meaningless attempts to access its data, including ePHI, makes it impossible for NTT DATA to report such unsuccessful Security Incidents in real-time or on any regular basis. Accordingly, Customer and NTT DATA agree that this provision constitutes timely notice to Customer of unsuccessful Security Incidents, whether occurring now or in the future, when they do not result in actual unauthorized access, use, disclosure, modification or destruction of ePHI or interference with an information system that contains or processes ePHI, such as but not limited to the following: i) pings on the firewall; ii) attempts to logon to a system, device or database with an invalid password or user name; iii) denial of service attacks; or iv) port scans.

- **Compliance Audits**: NTT DATA shall make its internal practices, books and records relating to the use and disclosure of PHI available to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining Customer's compliance with HIPAA.

- **Designated Record Sets**: If NTT DATA maintains any Designated Record Sets containing PHI, upon NTT DATA's receipt of a request from Customer for access to PHI about an Individual contained in any Designated Record Set(s) maintained by NTT DATA, NTT DATA shall allow Customer to access such Designated Record Set(s) in the manner originally received by NTT DATA and in the format and on the media in use as of the date of the request in order for Customer to meet its obligations to (a) make the PHI available in accordance with 45 CFR Section 164.524; and (b) amend the PHI in accordance with 45 CFR Section 164.526. As between Customer and NTT DATA, Customer, not NTT DATA, is responsible for responding to requests for access to or amendment of PHI from Individuals pursuant to HIPAA and the HIPAA Privacy Regulations, including, but not limited to, 45 C.F.R. §§164.524, 164.526, and 164.528, as the same may be amended from time to time. If NTT DATA uses or maintains an Electronic Health Record with respect to PHI, in accordance with Section 13405(e) of the HITECH Act, NTT DATA acknowledges that an Individual has a right to obtain from Customer a copy of such information in an electronic format. If the Individual makes an election to obtain from Customer a copy of such information in an electronic format, upon NTT DATA's receipt of written notice from Customer, NTT DATA will as

soon as reasonably practicable allow Customer to access any such information in electronic format so that Customer may provide a copy of such information in an electronic format to Customer.

- **Accounting of Disclosures**: NTT DATA shall document disclosures of PHI it makes and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of such disclosures in accordance with 45 CFR § 164.528; provided, however, with respect to disclosures made at the request of Customer under the Services Description, Customer shall be responsible for recording and tracking any such disclosures required by 45 CFR § 164.528. Upon NTT DATA's receipt of written notice from Customer that Customer has received a request for an accounting of disclosures of PHI regarding an Individual, NTT DATA shall make available to Customer the information collected by it as described above to permit Customer to respond to such request in accordance with 45 CFR § 164.528.

- **Minimum Necessary and Limited Data Set**: As described in 45 C.F.R. § 164.502(b)(1), when using or disclosing PHI or when requesting PHI from Customer (except for the uses and disclosures described in 45 C.F.R. § 164.502(b)(2)), NTT DATA will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. NTT DATA shall be treated as being in compliance with 45 C.F.R. § 164.502(b)(1) only if NTT DATA limits such PHI, to the extent practicable, to the limited data set (as defined 45 C.F.R. § 164.514(e)(2)) or, if needed by NTT DATA, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively. NTT DATA will determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

- **Marketing Use of PHI**: Except as provided in Section 13405(d)(2) of the HITECH Act, NTT DATA will not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless Customer has obtained from the Individual, in accordance with 45 C.F.R. § 164.508, a valid authorization that includes, in accordance with such section, a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual. Nothing in this Section 9 shall be construed to allow NTT DATA to disclose PHI except as provided in other provisions of this BAA.

- **Mitigation**: NTT DATA shall mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI by NTT DATA in violation of its obligations set forth in this BAA.

- **Consent, Authorization, and Permission**: Customer shall obtain and maintain such consents, authorizations and/or permissions, if any, as may be necessary or required under HIPAA, the HITECH Act, or other local, state or federal laws or regulations to permit Customer to disclose PHI to NTT DATA in order for NTT DATA to use and disclose PHI as required or permitted under this BAA. Customer shall promptly inform NTT DATA in writing as soon as Customer becomes aware of any modifications to, restrictions on, defects in, or revocation or other termination of effectiveness of, any such consent, authorization or permission, to the extent any such modifications, restrictions, defects, revocations or terminations affect NTT DATA's permitted or required uses and disclosures of PHI specified in this BAA.

- **Limitations in Privacy Practice**: Customer shall notify NTT DATA in writing of any limitation(s) in its notice of privacy practices in accordance with 45 CFR §164.520, to the extent any such limitations affect NTT DATA's permitted or required uses and disclosures of PHI specified in this BAA.

- **Uses or Disclosure Restrictions**: Customer shall notify NTT DATA in writing of any restriction(s) to the use or disclosure of PHI that Customer has agreed to in accordance with 45 CFR § 164.522,

to the extent any such restrictions affect NTT DATA's permitted or required uses and disclosures of PHI specified in this BAA.

- **Non-Permitted Use**: Without limiting Sections 1(a) – (e), Customer agrees it will not request, and the performance of NTT DATA's obligations under the Services Description will not require, NTT DATA to use or disclose PHI in any manner that would not be permissible if done by Customer.

- **Right to Terminate for Breach**: If NTT DATA commits a material breach of its obligations in this BAA, Customer may (a) terminate the Services Description (and this BAA) by providing NTT DATA prior written notice if NTT DATA fails to cure such breach within thirty (30) days of its receipt of written notice from Customer specifying the nature of such breach; (b) immediately terminate this Services Description (and this BAA) by providing NTT DATA prior written notice if a cure of such breach is not possible; or (c) report such breach to the Secretary if termination of the Services Description is not feasible.

- **Effects of Termination**: Upon the termination of this BAA for any reason, NTT DATA shall destroy or return all PHI in its possession by allowing Customer to retrieve any PHI uploaded to Dedicated Cloud, in accordance with the terms of a separate services agreement between Customer and NTT DATA and neither NTT DATA, nor its affiliates or their respective subcontractors shall retain copies of such PHI; provided, however, that if returning or destroying such PHI is infeasible for NTT DATA, NTT DATA shall extend the protections of this BAA to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible for so long as such PHI is maintained by NTT DATA.

- **Amendments**: The references to the provisions and sections of HIPAA and the HITECH Act in this BAA specifically refer to such provisions and sections as of the Activation Date, and do not include any amendments or changes to such provisions or sections enacted after the Activation Date or any guidance issued by a governmental entity after the Activation Date (including guidance issued pursuant to the HITECH Act). If any final amendments to HIPAA or the HITECH Act are enacted, or any governmental guidance is issued, after the Activation Date, to the extent such amendments or guidance require modifications to the then-current obligations of Customer or NTT DATA under this BAA, Customer and NTT DATA agree to promptly meet and negotiate in good faith to mutually agree on such modifications. Any material modifications to NTT DATA's obligations under this BAA may include changes in financial terms as reasonably required to support such cost of compliance.

- **Conflicts**: If there is any conflict between the terms of this BAA and the terms of the Service Description respect to the matters covered in this BAA, the terms of this BAA shall control.

HIPAA Safeguard Responsibility Matrix

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

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

Appendix F: PCI DSS Framework

The PCI Security Standards Council offers robust and comprehensive 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 robust 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 Customer.

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 3.0		
Dedicated Cloud - Base IaaS Service		
Responsible Entity • NTT DATA - NTT DATA is solely responsible • Both - Customer 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 Customer. • Customer - Customer 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. Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.	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. Customers 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. (For example, block traffic originating from the Internet with an internal source address.)	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. Note: Methods to obscure IP addressing may include, but are not limited to: · Network Address Translation (NAT) · Placing servers containing cardholder data behind proxy servers/firewalls, · Removal or filtering of route advertisements for private networks that employ registered addressing, · Internal use of RFC1918 address space instead of registered addresses.	NTT DATA & Customer	NTT DATA manages Customer 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. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	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—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.	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	

Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.		
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 · A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Customer NTT DATA	The Customer 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 in accordance with customer 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:	Customer	
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. Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained: · The cardholder's name · Primary account number (PAN) · Expiration date · Service code To minimize risk, store only these data elements as needed for business.	Customer	
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.	Customer	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	Customer	
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. Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.	Customer	

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. Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	Customer	
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	Customer	
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.	Customer	
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	Customer	
3.5.2 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 Note: It is not required that public keys be stored in one of these forms.	Customer	
3.5.3 Store cryptographic keys in the fewest possible locations.	Customer	
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.	Customer	
3.6.1 Generation of strong cryptographic keys	Customer	
3.6.2 Secure cryptographic key distribution	Customer	

3.6.3 Secure cryptographic key storage	Customer	
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).	Customer	
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. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes	Customer	
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	Customer	
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	Customer	
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Customer	
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Customer	
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.	Customer & NTT DATA	NTT DATA is responsible for assisting with the configuration of VPN connectivity. All other cardholder data encryption in transit is the responsibility of the Customer.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control is prohibited.	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.).	Customer	
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.	Customer	

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. Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.	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. Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization’s environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a “high risk” to the environment. In addition to the risk ranking, vulnerabilities may be considered “critical” if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.	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	Both	

within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.		
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.	Both	create policy
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to Customers.	Both	
6.3.2 Review custom code prior to release to production or Customers 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. Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	Both	
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	Customer	
6.4.4 Removal of test data and accounts before production systems become active	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	

6.5 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 Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	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 Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. · Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic	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 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance) Note: Two-factor authentication requires that two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication. Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.	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 Customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each Customer.	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	Both	

· Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access		
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)	Customer	
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 - Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)	NTT DATA	
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	Customer	
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). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.	Customer	

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).	Customer	
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. Note: One example of time synchronization technology is Network Time Protocol (NTP).	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. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	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).	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 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. Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.	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). Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed. For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if	Both	

the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.		
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. Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan Customer responsibilities, scan preparation, etc.	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 · Specifies retention of penetration testing results and remediation activities results.	Both	
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	Both	

segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		
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. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	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.), · Identifies critical assets, threats, and vulnerabilities, and · Results in a formal documented analysis of risk. Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	Both	
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage. 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.	Customer	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	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 importance of cardholder data security.	Both	
12.6.1 Educate personnel upon hire and at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	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.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	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 Customer, or to the extent that they could impact the security of the Customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	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 Customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the Customer, or to the extent that they could impact the security of the Customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	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	
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. Note: Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.	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 Customer's virtual environment - this remains a Customer 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 G: Internet Service Options

Committed Bandwidth with Optional Burst

Introduction to Committed Bandwidth

NTT DATA Committed Bandwidth Internet Services (the "Internet Service") provide Customer with committed internet bandwidth and, if purchased, burst bandwidth capability, so that Customer can access its Dedicated Cloud Service.

Offer Description

Service Offer

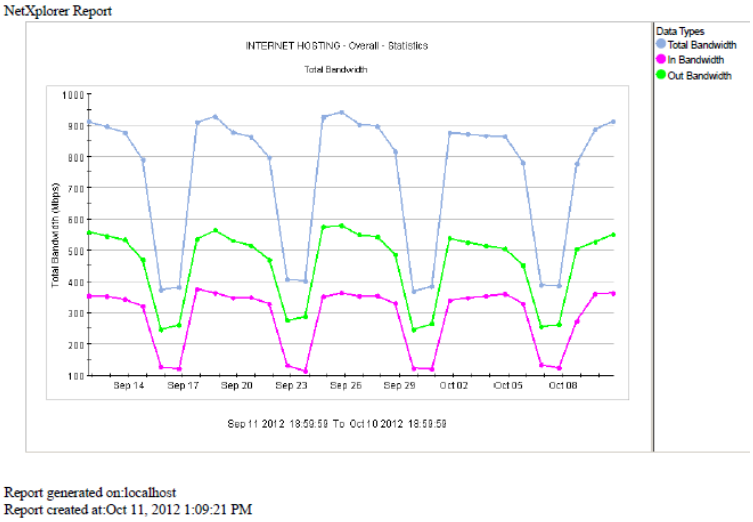
In order to provide Internet access to your content in your Dedicated Cloud environment, you will require internet bandwidth. You should work with your NTT DATA account representative to determine the amount of internet bandwidth required for your particular use cases.

Internet Service details and options are listed below.

Service Details –Committed Bandwidth
Dedicated Internet Bandwidth • Provided by the Mbps • Provided by multiple carriers • Capped at the dedicated amount that Customer has requested. For example, a 5MB dedicated bandwidth will start to experience performance degradation as the throughput exceeds the threshold that has been set • Billed on a monthly basis at the rate procured • Adjustable to accommodate peak load times in the week, month or year
Incoming Network Traffic Load Balancing (different from Dedicated Cloud Load balancing service) • Available for incoming traffic from the Internet • Allows for load balancing across virtual servers in Customer's Cloud environment • A leveraged managed service • Requests for Move/Add/Change/Deletes (MACDs) are submitted via the service desk for the Dedicated Cloud service
Optional Burst provides burst Bandwidth capability • This is NOT a metered service • The burst bandwidth is purchased at a static rate, for example, 5Mbps burst. • Optional Burst bandwidth is not dedicated; rather burst bandwidth includes shared traffic. Accordingly, performance degradation may occur when Customer is utilizing Optional Burst bandwidth
Reporting

- Bandwidth-related reporting is sent to the Customer-provided email address, that has been assigned to the account
- Reported frequency is determined by Customer, as reports are generated automatically and sent to Customer via email

Below is a sample report:



- Quality of Service (QOS) is not available as NTT DATA cannot control the availability or prioritization across the internet

Appendix I: NTT DATA Dedicated Cloud Colocation Services

NTT DATA is pleased to offer Colocation Services in 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 Customers 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 Customer's purchase of Colo Services.

Offer Description

The Dedicated Cloud Colo Service is a supplementary service intended to provide the Customer with rack space, power, cooling and physical security for Customer'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 Customer's Dedicated Cloud instance(s). This Colo Service requires, but is not limited to, the following high level process steps:

- Customer configures Equipment with IP addresses from Customer assigned pool of addresses from the Dedicated Cloud
- Customer 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 Customer's Dedicated Cloud environment
- NTT DATA personnel power up Equipment and notify Customer 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 Customer at Customer-provided shipping address

As necessary, NTT DATA will assist Customer to resolve local Equipment issues with vendor access to equipment at Data Center. Customer agrees that Customer 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 Customer 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.

Customer-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 Customer equipment does not meet these specified requirements or if Customer 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 Customer at Customer-specified shipping address, at the Customer’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 Customer 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 Customer’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 Customer for management of installation and maintenance of Customer’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 Customer Equipment to the Dedicated Cloud environment. Can be done for single or redundant network connections. • Colocation electrical connections if Customer Equipment only has one power connection; there is an additional charge for an electrical transfer switch. • 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 Customer 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 Customer 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 Customer, 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

Customers 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 will be included in the standard service charge for Colo Services to the Customer.

Offer Description

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

- Customer ships Equipment, and necessary peripherals as outlined below, to Data Center.
- NTT DATA receives Equipment and installs in a Data Center.
- Power and network/fiber cables are connected to Equipment in the cabinet(s).
- Equipment is connected to Customer's location with Customer provided network circuits or NTT DATA Internet bandwidth.
- NTT DATA personnel power up Equipment and notify Customer 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 Customer at Customer-provided shipping address.

As necessary, NTT DATA will assist Customer to resolve local Equipment issues with vendor access to devices at the Data Center. Customer agrees that Customer 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 Customer Equipment utilized for the Dedicated Cloud Colocation Service to reduce risks of data compromise during shipment to and from the Data Center.

If Customer 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 Customer at Customer-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 Customer for management of installation and maintenance of Customer'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 Customer provided network switches to the Customer 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 Customer provided fiber switch to Customer 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 Customer's equipment. Sold per hour increments.

Customer Responsibilities

The following Customer Responsibilities apply to all Dedicated Cloud Colo Services.

- Prior to purchasing the Colo Service Customer must have purchased Dedicated Cloud services from NTT DATA.
- Customer will configure the Equipment to be installed into the Data Center and will configure the Equipment for particular applications.
- Customer will load the Customer application and databases on the Equipment and ship the Equipment to NTT DATA using the address and shipping information provided.
- Customer is responsible for shipping the Equipment from NTT DATA datacenter at Customer's cost. A pre-paid return shipping label must be included and provided by the Customer.
- Customer will encrypt its data on the Equipment before shipping to NTT DATA.
- Customer is responsible for the network routing of its server into its Dedicated Cloud environment once installation is complete.
- Customer represents and warrants that it has obtained permission for both Customer and NTT DATA to access and use, whether remotely or in-person, Customer-owned or licensed software, hardware, systems, the data located thereon and all hardware and software components included therein, for the purpose of providing the Colo Service. If Customer does not already have that permission, it is Customer's responsibility to obtain it, at Customer's expense, before Customer asks NTT DATA to perform the Colo Service.
- Customer 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. Customer 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.
- Customer 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. Customer 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 Customer. 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 Customer Equipment is at the expense and risk of Customer. NTT DATA is not liable for any data loss as a result of the de-installation or shipping process.

Insurance

Customer 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 Customer's public cloud solution or environment
- Data design

- Synchronization of the Customer's application and database with Customer'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 Customer Equipment-based data
- De-installation of Equipment
- Special projects for any physical adds/moves/changes or deletes or custom reporting

Appendix J: NTT DATA Managed Cloud Services

Customer has the option to purchase NTT DATA Managed Cloud Services in addition to Dedicated Cloud Services. Managed Cloud services offers three service coverage levels:

- Cloud Monitoring and Alerting (CMA)
- Cloud Monitoring and Remediation (CMR)
- Cloud Operations Management (COM)

The table below presents a combined view on solution features available for each different service coverage level.

	Cloud Monitoring and Alerting	**Cloud Monitoring and Remediation**	**Cloud Operations Management**
1. Cross Cloud Compatibility	✓	✓	✓
2. Portal access	✓	✓	✓
3. Alert Dashboard	✓	✓	✓
4. Visibility and audibility	✓	✓	✓
5. Standard Monitoring	✓	✓	✓
6. Advance monitoring		✓	✓
7. Alert Management		✓	✓
8. Preventive Maintenance		✓	✓
9. Standard Operating Procedure (SOP) based mediation		✓	✓
10. Troubleshooting with full remediation			✓
11. Root cause analysis of critical incidents			✓
12. Preventive health checks			✓
13. Move, Add and Changes (MAC) and Service Request (SRs)			✓

These services are available under a separate service description from NTT DATA at an additional charge.

Additional information on 'Managed Cloud Services' can be found at https://www.nttdataservices.com/-/media/nttdataservices/files/contracts/saas-and-cloud-services/ntt-data-managed-cloud-services.pdf?la=en-us.

Appendix K: Disaster Recovery (DR) Service

Introduction to Cloud Disaster Recovery Service

The Disaster Recovery Service (the "DR Service") is a Customer-managed disaster recovery service whereby will provide a disaster recovery technology integrated to the Customer'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 Customer's VM environment to an alternate site based on a Customer-defined disaster recovery plan.

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

NTT DATA will use Recovery Point Objective (RPO) and Data Change Rate information from the Customer 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 Customer managed self-service offer. Therefore, the Customer maintains control and responsibility for defining, implementing and maintaining recovery plan along with RTO targets unless the services are contracted as add-on service to NTT DATA under an 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 Customer's production environment.

Infrastructure supporting the DR Services is subject to same SLA criteria as mentioned 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 Customer'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 Customer data (via shipping of data on hard drive from Customer 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
- Proof of concept test using NTT DATA's "Hello World" DR template

Post implementation Assistance

Any post implementation DR project based work covering assistance in activity 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 L: Data Protection (backup) Service

Introduction to Data Protection (backup) Service

Data Protection (backup) Service allows Customer to perform backups on its own terms and retain backups for as long as required according to Customer's internal data retention policies.

Service Offer

NTT DATA will work with the Customer to setup and configure the data protection service including Dedicated Cloud backup scheduling solution and the web portal to monitor distributed back-up jobs in a single plane of glass. Once the solution is set-up NTT DATA will provide a brief orientation and detailed instructions to the Customer to enable Customer operate the back-up solution in a self-service manner.

Offer includes

- Infrastructure required for hosting the back-up application
- Windows Guest OS and back-up application licensing required for the back-up solution
- One or more back-up applications that perform the back-up jobs
- Web based dashboard for consolidated view to monitor distributed back-up jobs
- Help with the initial set-up of the back-up solution
- Basic orientation training of the back-up solution
- Documentation required to configure and run back-up jobs in a self-service manner
- Optionally second cloud site and connectivity required to meet second site data back-up needs

Customer Responsibilities

- Design and implement backup jobs that meets the needs of the business using Dedicated Cloud Back-up offering
- Monitor scheduled backup activity regularly, and verify successful completion
- Remediate back-up failures
- Monitor back-up storage capacity. Request additional capacity from NTT DATA using the Service Request process
- Restore VMs or files as needed

Appendix M: Cloud Management Platform Service

Scope

The Cloud Management Platform (CMP) shortens the time required to provision infrastructure from days to hours through automation of IT service delivery and enables efficient management of private, public and hybrid clouds. CMP consists of an intuitive portal empowering administrators and users to request and a manage variety of 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 IT Service Management (ITSM) tools. CMP enables governance of access and cost controls across public and private clouds. CMP is powered by VMware vRealize Automation (vRA) and VMware vRealize Orchestrator (vRO). NTT DATA also enables representational state transfer (REST) application programming interface (API) access to vRA which can enable automated provisioning of virtual servers trigged by another system.

Definition of Terms

These terms are used within this document.

vRA	VMware vRealize Automation
vRO	VMware vRealize Orchestrator (formerly vCenter Orchestrator)
Blueprint	VMware vRealize Automation Blueprint
Catalog Item	VMware vRealize Automation Catalog Item
Workflow	VMware vRealize Orchestrator Workflow

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-Customer vRA and vRO environments managed by NTT DATA and thirty (30) hours of remote consulting during onboarding to provide a Service that conforms to individual Customer requirements.

Additional development efforts beyond the initial 30 hours must be scoped and purchased separately. NTT DATA will only provide support for both the vRA and vRO base configuration along with any NTT DATA covered Blueprints, Catalog Items and Workflows. The base package requires that NTT DATA maintains administrative rights within vRA and vRO.

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

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

	Base Package
1. Initial Customer configuration	Included
2. Development of Blueprints, Catalog Items and Workflows	Up to 30 hours included

3. Leveraging NTT DATA knowledge repository to accelerate Customer specific development	Included
4. vRA and vRO license	Included
5. Break fix support	Included
6. Backup and Restore for vRA and vRO	Included
7. Upgrading and patching	Included
8. Service Requests (SRs)	Included
9. Incident Acknowledgement Time and Incident Resolution Time SLAs	Included
10. Ability to manage non-Dedicated Cloud environments	Optional
11. Cloud Management Platform consulting	Optional

1. Initial vRA and vRO Customer configuration

Base package is limited to one (1) tenant in a secure multi-Customer vRA environment and one (1) tenant in secure multi-Customer vRO environment. Multi-Customer vRA environments and multi-Customer vRO environments are provisioned outside of the Customer's environment.

The initial vRA and vRO configuration service includes:

- Requirements gathering
- Provisioning tenants within vRA and vRO
- Base configuration of vRA and vRO within standard functionality
- Work instructions
- Transition training delivered remotely, lasting up to two (2) hours maximum.

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

2. Development of Blueprints, Catalog Items and Workflows

NTT DATA will provide a maximum of (30) hours of Cloud Management Platform consulting services to assist the Customer 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. Additionally, 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. Customer sign-off and acceptance

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

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

4. License Requirements

Both the vRA and vRO license costs are included within the CMP services agreement.

5. Break-fix support

NTT DATA will provide break-fix support to Customer vRA and vRO environments. Break-fix support is limited to:

- base vRA configuration.
- base vRO 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. Backup and Restore for vRA and vRO

NTT DATA will perform a daily backup of Customer vRA and vRO environments. NTT DATA will perform recovery of Customer vRA and vRO environments as needed.

7. Upgrading and Patching

NTT DATA will maintain vRA and vRO patch and update compliance through an internal control process on behalf of the Customer. 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 vRA and vRO environments using best practices.

8. 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 Service Now. 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 leverage the Incident Acknowledgement Time and Incident Resolution Time SLAs as defined in Appendix A.

9. Incident Acknowledgement Time and Incident Resolution Time SLAs

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

10. Ability to Manage non-Dedicated Cloud Environments

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

11. 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
- vRA enhancements
- Workflow development and customizations
- vRO enhancements

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 N: Dedicated Cloud Encryption Protection

Introduction to Dedicated Cloud Encryption Protection

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

- **Installation & Configuration**: – As part of onboarding the Customer 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 Customer on the Dedicated Cloud environment, NTT DATA will provide a permanent license file to the Customer and the Customer 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 Customer of available software updates. It will be up to the Customer to decide when and which software (key management server, transparent agent, application agent) to update at the Customer's cost.

Customer Responsibilities

- **Set Access Policy**: Customer must develop their own access policy and configure the key management server according those policies. Customer 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 Customer Encryption Policy** – Customers are responsible for maintaining their encryption policies.
- **Audit & Reporting** – Customers are responsible for generating reports from the key management tool and performing required audit.

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

Category	Activity	NTT DATA	Customer
Customer Onboarding	Provision VM for Key Management	X	
Customer Onboarding	Create License file	X	
Customer Onboarding	Initial Installation of the Key Management software	X	
Customer Onboarding	Configure Firewall	X	
Customer Onboarding	Configure Change Auditor for Key Management alerts	X	
Customer Onboarding	Configure Key Management software		X
Level 1 Support	Answer to a Customer 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	Adding and deleting domains		X
Administration	Assigning administrators to domains		X
Administration	Configuring Key Management preferences and logs		X
Administration	Backing up and restoring the Key Management database		X
Administration	Configuring high availability		X
Administration	Configuring syslog servers for system-level messages		X
Administration	Installing the license file		X
Administration	Viewing and downloading system-level reports		X
Administration	Notify Customer of Key Management software updates	X	
Administration	Updating Key Management software		X
Administration	Adding and removing Key Management administrators in domains		X
Administration	Configuring syslog server for application-level messages		X
Administration	Viewing and downloading domain-level reports		X
Administration	Viewing Key Management preferences and logs		X
Administration	Creating and configuring signature sets		X
Administration	Configuring keys and key groups		X
Administration	Configuring online and offline policies		X
Administration	Configuring protected hosts and host groups		X
Administration	Sharing a host with another domain		X
Administration	Exporting and importing keys		X
Administration	Viewing Key Management security administration preferences and logs		X