Cloud Services Division Client Service Description

1 Cloud Services

The following are common services to all NTT Cloud Services products and describe the in-scope items for the Services attached to this Client Service Description.

1.1 Technology Standards

NTT has developed standard offers for our entire service portfolio which provide specific monitoring configurations, Service Requests and Transition tasks for supported technologies. These technology specific standard offers are described in the specific Service Description(s) attached to the SOW. NTT may revise the Service Description(s) at any time by notice to the Client.

1.2 Language Support

Support services are in English unless otherwise specified in the Statement of Work. All supported operating systems, software, firmware, and related documentation, including but not limited to Client or third-party provided documentation, runbooks, and other related materials must be in English.

1.3 Client Responsibilities

In addition to any Client responsibilities identified in subsequent sections of this document and the service description(s) attached to the SOW, the following are Client responsibility:

(a) All required consent, authorization, license, use rights, software licenses, required for NTT to perform the Services, unless otherwise specified in the Software Responsibilities Table of the SOW.

(b) Except for solutions hosted on NTT Private Cloud (multi-tenant), tasks requiring physical access (for example, installation of physical devices)

(c) Hardware and software maintenance contract (with NTT or OEM vendor) that matches the SLO of the service (e.g., 24/7/365 with 4-hour on-site support)

(d) Any task which requires physical access; provision/procurement of “smart hands” support (i.e., physical restart of a device is required); per individual Agreement, this may be outsourced to NTT or another vendor

(e) Any Disaster Recovery or Disaster Recovery Management is out of scope, unless specifically identified as In-Scope in the SOW for the relevant Service.

(f) Provide NTT the required access and connectivity as determined by NTT

(g) Any task or activity within a Service Description not specifically identified as In-Scope in the Statement of Work

1.4 NTT Information Security Management System

To assure the confidentiality, privacy, integrity, and availability of information assets belonging to NTT and its clients, NTT has an information security program which consists of policies, processes, and procedures that build and fulfil the requirements of NTT’s Information Security Management System. For some contracts, this information security program replaces the document known as the “Secure-24 Security Protocol.”

2 Service Delivery Process

2.1 Service Coverage

NTT provides the following options:

(a) **Full Coverage (24x7):** Full coverage is typically used for production environments, providing 24x7 incident resolution and the highest level of service guarantees.

(b) **DR Coverage:** Disaster Recovery (DR) coverage is intended for the management of redundant IT architectures, which are maintained in *standby* mode and are used only when a system's primary architecture fails. DR coverage provides Full Coverage services only when the redundant architecture is Note: Client must have a DR solution in Scope. If NTT has been contracted to provide Managed Disaster Recovery services, the Client is responsible for invoking DR site failover.
The specific coverage option selected is specified in the SOW.

2.2 Service Management Frameworks

ITIL v4 and ISO 20000 are the global de facto frameworks for IT Service Management best practices and NTT service delivery process are structured to be directionally aligned. As such, NTT service delivery comprises:

(a) Service asset and configuration management

(b) Event management

(c) Incident management

(d) Problem management

(e) Request fulfilment

(f) Change management

(g) Continual Service Improvement

(h) Service Level Management

(i) Access management

(j) Availability and capacity management

As part of service transition, NTT works with the Client to identify how best to interlock operational processes.

2.3 Service Asset and Configuration Management

NTT maintains a Configuration Management Database (CMDB) for the CI's in Scope and under management for the Client and updated by NTT based on Change Management or Service Requests and NTT's automated process which may be performed by auto-discovery and other CMDB enrichment tools.

2.4 Event Management

NTT will provide monitoring services for systems under management, using technology specific Standard Monitoring configurations, unless otherwise specified in the SOW.

Monitoring will be performed at a set frequency as specified in the SOW or Service Description. If an anomaly is detected, the system will recheck twice automatically and, if the anomaly is persistent, generate an alert. For the purposes of SLA availability calculations, downtime will start after the second recheck.

The response to monitoring alerts will be as follows, depending on the criticality and expected associated action:

Alert Response	Output
No alert, data only	The monitor does not generate an alert nor an Incident ticket. The data is collected only for informational purposes.
Priority 1, Priority 2, Priority 3, Priority 4	This will generate an alert ticket that will be managed by the operations team.
Solution Monitor	Generates an alert which is immediately escalated to a P1 Incident ticket. Solution Monitors are configured for measuring the availability of the Client application Applicable only when management of Client applications are in-scope

Once an alert ticket is generated, NTT engineers will review the alert and:

(a) If the monitor that triggered the alert has returned to normal values, the alert is cleared, and no Incident ticket is created.

If the re-test fails, an Incident ticket is generated with the associated severity and Incident Management activities will be initiated.

2.5 Incident Management

(a) Prioritization of Incidents

Incident tickets will have a priority assigned to them which is determined by the impact and the urgency of the Incident.

NTT will assign the right priority by assessing the impact and urgency of the Incident ticket.

The table below illustrates how priorities are assigned to Incident tickets:

Priority		Impact			
		High	Medium		Low
		The majority of users of the service or the majority of users in a single central office are, or have the potential to be, affected. Workaround is not available.	Some users are, or have the potential to be, affected. A workaround may or may not be available.		Minimal number of users of the service are, or have the potential to be, affected. A workaround is available.
Urgency	High	The issue has caused a work stoppage, or has the potential to cause a work stoppage, of a vital business function or service. This includes a degradation of service to a point in which the user is unable to perform normal business operations. These	Critical (P1)	High (P2)	Medium (P3)

		include external communications or processes that impact revenue creation.			
	Medium	The issue has not resulted in a work stoppage but has impaired the user's ability to perform their normal business operation.	High (P2)	Medium (P3)	Low (P4)
	Low	The issue has not impeded or disrupted the normal business operations.	Medium (P3)	Low (P4)	Low (P4)

The urgency and the impact of a ticket will be assigned based on the table above in NTT's reasonable discretion, and may be applied automatically by the alerting mechanism, based on the associated monitoring.

(b) Incident Resolution

NTT will assess the impact of an Incident, notify the Incident owner, troubleshoot, and attempt to resolve Incidents reported by the Client.

When NTT has resolved an Incident, NTT will set the Incident ticket to "resolved" and notify the Client. Client shall then confirm that the Incident has been resolved, and "close" the ticket, or respond to NTT with further information. In the event the CI is maintained by a third party of the Client, NTT will refer the incident to the Client (for example, a third party provided public cloud that NTT provides management).

(c) Inactive Tickets

During the resolution of Incidents, it may be necessary to obtain additional information or actions from the Client. While waiting for the Client response, work on the Incident may be halted.

Incidents without a response from the client are eventually closed. Our support team will update the ticket requesting the client's response three (3) times, over a three (3) to six (6) day period. After the third failed attempt the ticket will be set to a resolved state. If the client does not reactivate the ticket after three (3) days, the ticket will be automatically closed.

In the event that NTT receives an automated out-of-office response when attempting to contact the Client, the ticket will be suspended and no work shall continue until the Client's return date.

Incidents with impact where the Client does not cooperate in its closure will be registered as risks and closed. Should the monitoring continue to generate Events due to the unresolved Incident, the related monitoring will be suspended until the risk is mitigated.

(d) Major Incident Management

Under certain conditions, NTT may upgrade a P1 Incident to a Major Incident, invoking the Major Incident Management process. During this process, multiple engineering teams may be involved in the problem resolution and the Client is notified of the resolution progress.

A P1 Incident will become a Major Incident when one or more of the following apply:

(i) The Client declares that there is a service interruption in one of the critical business functions (Business Services) that has a production and or financial impact to the business

(ii) The issue is impacting 10 or more end-users

or when a P1 Monitoring Ticket (incident detected by the monitoring and event management system), then:

(iii) NTT will validate the impact of the Incident and declare it as a Major Incident in NTT's discretion.

Incident Report (Major Incidents)

As part of the Major Incident Management process, an Incident Manager will be assigned to coordinate the different teams involved in the troubleshooting, drive the service restoration, and ensure proper communication to internal and external stakeholders. Once the service has been restored and the Client has confirmed that there is no further business impact the outage will be considered resolved. NTT's Major Incident Management team will document the Incident in an Incident Report with the intent to deliver it within 5 business days.

(e) Disaster Recovery

If NTT has been contracted to provide Managed Disaster Recovery services, the Client is responsible for invoking DR site failover. NTT will provide any available information to assist the Client with the decision-making process.

2.6 Problem Management

Problem Management is the process of identifying the underlying causes of an Incident and establishing a formal process for resolution.

Problem Management will be initiated in one of two ways:

(i) Reactive Problem Management: initiated in response to an Incident where the root cause is unknown and only applies to Major Incidents, P1 incidents resolved with unknown root cause, or P2 Incidents resolved with unknown root cause as requested by the Client.

NTT's engineering teams will attempt to determine the root cause for the problem. Once this is done, the Knowledge Management process will be invoked to update runbooks and document the problem and solution.

(ii) Proactive Problem Management: initiated as a result of the analysis of repetitive alerts and recurring Incidents, for Technology related issues the Technology Team will own the problem until its resolution, and for Client solution related issues: the applicable Engineer within the POD or Team will help ensure that the root cause is identified, and the Client is notified. If the Client refuses to collaborate on resolving an issue, NTT reserves the right to suspend monitoring and the SLA of the affected Components or Configuration Items.

2.7 Request Fulfilment

A Service Request is a ticket that contains a request for information, advice or a change which is within the scope of contracted NTT Cloud Services. This is distinct from the response to alerts or urgent change requests in response to Incidents.

(a) In-scope Service Request

Service Requests that are listed as a service request or activity in the applicable service description are considered "in-scope" and therefore, do not incur Client charges up to any limit specified therein. These requests will be processed after NTT has received all relevant information deemed necessary by NTT to complete the request. A list of In-scope Service Requests for specific technologies is included in the relevant service descriptions in the applicable SOW.

(b) Out of Scope Request

If NTT determines that the Client has requested activities in its reasonable discretion which are not in-scope, the following process will apply:

(i) NTT will notify the Client that the request is not in-scope and therefore, it will be chargeable

(ii) If the requested activities are chargeable, NTT will notify the Client. NTT will present the Client with the charges in accordance with the MSA Change Order Process.

(iii) Once written approval is received, NTT engineers will proceed with the request

(c) Limitations for Service Requests

NTT reserves the right to suspend or re-schedule any request that implies an interruption of the service, and therefore needs to be resolved within a maintenance window.

NTT reserves the right to suspend any service request that implies a change to the scope of any of the contracted managed services. Such changes include, but are not limited to:

(i) Installing new software

(ii) Changes to the monitors required

(iii) Addition/removal of a server or other platform element

(iv) Changes to the network architecture

Such Service Requests will be treated as a new project and will be subject to additional fees.

(d) Fair Use Policy

NTT employs a "Fair Use" policy that reserves the right to limit the number of in-scope service requests during an extended timeframe. Unless this policy is invoked, there is no limit to the number of in-scope service requests generated by the client.

The following is a non-exhaustive example of practices considered a violation of the Fair Use Policy:

(i) the number of concurrent service requests opened by Client exceeds the maximum of 3 + 1 (rounded up) for every 10 configuration items under management

(ii) the level of effort required to resolve Service Requests exceeds 1 hour per month for every 10 configuration items under management

(iii) the number of requests to restore from backup is limited to one restore per endpoint per week per 100 endpoints.

At its discretion, NTT reserves the right to invoke the Fair Use policy, and to review and limit its provisions of requests or to upgrade the Client to a different service more suited for Client's usage. In extreme cases, NTT may, with reasonable notice, suspend or terminate the Client's ability to use the Service.

2.8 Change Management

A Change is any addition, modification, or removal, of configuration items that could affect live services. This is the internal process for change management. Contractual change management may be required as per the MSA before any change may be executed in NTT's sole and absolute discretion. Client can submit a request for change via the Services Portal or NTT can define the need for a Change as a means to resolve an Incident, a Service Request, or a Problem. The process for change management shall be determined by the Master Services Agreement.

NTT provides 24x7 coverage for Emergency Incident-related Changes, and coverage within business hours for standard and normal Changes.
Changes can be scheduled outside of business hours (OOBH) but may be subject to additional charges, and are subject to the below requirements:

(i) All Changes that need to be performed Outside of Business Hours must be communicated to NTT with **at least 5 business days' notice**.

(ii) All non-emergency Change Requests require **at least 2 business days in advance to the Change owner**.

(a) Standard Changes

Changes with a level of complexity that meet the available technical skillset of NTT helpdesk support staff can be executed 24x7. All other Change Requests are subject to the OOBH requirements as described above.

2.9 Risk Management and Mitigation

As part of ongoing support, NTT will document all risks identified within the Client Solution and shall communicate those deemed relevant by NTT to Client.

(a) Risk Exceptions

Under certain conditions the Client may not agree to take risk mitigation actions as requested by NTT, or the Client may request NTT to take actions not advised by NTT. In such cases, NTT will notify the client of the risk, and some potential consequences of the action or non-action by issuing a Risk Exception notification. NTT may then agree to provide services against the impacted Service with Reasonable Effort (as defined below). By signing the SOW to which this CSD is applicable, Client acknowledges that if a Risk Exception is issued, the Reasonable Effort terms below shall override and supersede anything to the contrary in any of the applicable contract documents between the parties, including the Master Services Agreement, SOW, SLA, or any other applicable contract document.

(b) Reasonable Effort

Reasonable Effort is defined as delivery of services on a reasonable-effort basis, without any guarantee of success or acceptance of any liability, or responsibility for errors, loss, or issues which could have been avoided had requested actions been taken or avoided (as applicable).
Under Reasonable Effort the following shall apply:

(i) NTT's response to Incidents and Alerts will continue to be performed in alignment with the relevant criticality.

(ii) Service credits will not be owed for any missed SLAs against impacted services which occur while the exception is in place.

(iii) Monitoring and Alerts are enabled; however, NTT reserves the right to suspend Event Management activities in case of persistent issues caused by a Risk Exception.

(iv) If the resolution of an Incident requires more than 4 hours of troubleshooting, NTT reserves the right to charge the client for any additional effort at standard engineering hourly rates.

(v) NTT does not guarantee the security of any data, including but not limited to personal data, Client intellectual property, application configuration or code, related files, databases, or content, regardless of the security measures and configuration in place. The Client shall be fully responsible for the state and quality of any data or information or systems which are at risk due to the Risk Exception.

Should the Client wish to remove a Risk Exception, NTT reserves the right to conduct an inspection of the relevant systems to confirm their supportability. Inspections may result in additional charges to the Client.

2.10 Patch Management

(a) NTT Internal Systems and Infrastructure

NTT defines how and when patches are applied to NTT systems, devices, and applications.

(i) At its sole discretion, NTT will prioritize patches based on the importance of assets and the risk associated with the underlying vulnerability.

(ii) Except in the case of Emergency Patching, patches are deployed on a regular schedule at a maximum of once per month.

(iii) In cases where NTT has identified that the Client solution may be impacted by patch deployment activities on NTT internal systems and/or infrastructure, NTT will contact Client with a requested maintenance window; Client shall in good faith approve the maintenance window or provide an alternative window which is agreeable to both parties; if Client is unable or refuses to provide a maintenance window, NTT may, in its sole discretion perform patching without Client consent, as necessary to mitigate risks posed from not applying required patches.

(b) Client CIs under NTT Management

For Client CIs under NTT Management for which Patch Management is in scope NTT will apply the same above patch management methodology, unless, at the discretion of NTT, this methodology poses a risk or is incompatible with the Client's solution.
NTT recommends following a release management process that allows patches to be deployed into pre-production or test environments before deploying patches into production. This approach is intended to reduce,

as much as possible, the risk of a patch resulting in unexpected behavior, or that might result in an outage or Incident.

(i) Regularly Scheduled Patching
Regular patching is necessary as part of maintaining compliance with vendor support contracts. NTT, with the involvement of the Client, will establish a recurring maintenance window to apply vendor patches. See relevant technology specific services descriptions for patching schedule and further details.

(ii) Emergency Patches
Any patch which NTT determines carries too high a risk to address during the regularly scheduled patch window, can be issued as an Emergency Patch, following the Incident Management Process.

(iii) One-Time Patches
If needed as part of Incident Resolution, NTT may apply patches outside the normal recurring patch window, and without the Client approved patching window.

(c) Patch Management Client Responsibilities

(i) Clients must ensure their applications are safe for patching and all pending functional changes are complete. Client is responsible for application testing upon completion. Troubleshooting and break-fix services associated with Client applications/code are not in scope and Client responsibility.

(ii) Client will, in good faith, respond to requests for patch approval, and related maintenance windows in a timely manner. If NTT is unable to obtain timey responses from Client, and systems under management become out of date, NTT will issue the Client a risk exception. See the Risk Management and Mitigation section of this document.

(d) Patch Management Limitations

(i) If the Client rejects, or otherwise does not approve a patch request, then Client accepts responsibility for any risks covered by the patches that would have been applied, and any SLAs shall not apply.

(ii) If Client's solution provides no testing or preproduction environment, this serves as a default acceptance of risk of any outages or Incidents which result from patches or patch related activities taken by NTT, and any SLAs related to their remediation shall not apply.

(iii) Applying third-party or non-OEM vendor patches is not supported.

2.11 OS, System and Application Upgrades
Major upgrades subsequent to the installed release are out of scope. Depending on the software or system to be upgraded, NTT will provide a separate Statement of Work for the additional effort required to complete the project.

2.12 End of Life Technologies
NTT maintains a supported technology list within each applicable service description and does not support technologies or versions which have been deemed End of Life ('EoL') or End of Support ('EoS') by the technology vendor.
NTT will notify the Client as technologies become EoL, EoS or removed from NTT's supported technology list and provide them with a project plan to upgrade to the next recommended supported version at Client's cost. If the Client determines that it will not comply with upgrade recommendations, including the cost of the project to perform such upgrades, NTT will document this non-action as a risk, and issue the Client with a risk exception. See the Risk Management and Mitigation section of this document.

3 Service Management

The Service Management function is performed by the NTT Service Delivery Manager (SDM).

4 Platform Access & Operational Support Tools

4.1 Platform Access
To deliver the Service, the **NTT Operations Team must have remote access to the Client solution. This access requires from the Client a high level of availability, reasonable latency, and sufficient bandwidth.**

4.2 Identity and Access Management
Primary management activities will be performed from NTT's access management zones. Access management zones are remote access solutions that use multi-factor authentication (MFA).

4.3 Connectivity to the Client Environment
NTT requires that the connection from the NTT operations facility to the Client environment is performed over one or more of the following transports:

(a) An IPsec VPN tunnel established between the Client platform and NTT's access management This is the default option that provides encryption of all the communications from firewall to firewall:

(i) IPsec VPN must be routed with no network address translation (NAT) between NTT and the Client; IP ranges in the Client platform must be assigned by NTT

(ii) If IPs can't be assigned by NTT (for example if taking over an existing platform), NTT will require that destination NAT is configured at the Client-end. If this requirement cannot be met, NTT may determine that the solution cannot be supported

(b) An MPLS link between the Client platform and NTT's access management zones. This method is highly secure as it provides a private network. As communications do not flow through public networks, encryption is not mandatory unless otherwise stated by the Client. Additional setup and recurring charges will apply

(c) An SD-WAN solution with a virtual endpoint running within NTT's access management This method extends the Client's SD-WAN overlay network into NTT's management infrastructure and provides equivalent functionality to extending an MPLS link between the Client platform and the access management zone. Communications flowing over this type of link will be encrypted in line with the encryption offered by the SD-WAN vendor. Additional setup and recurring charges will apply.

The specific method of Connectivity shall be selected once after the execution of the SOW and may not be changed without a Change Order. NTT does **not** support the following:

(a) Client-owned MFA (multi-factor authentication) systems. NTT uses its own MFA methods.

(b) Client-to-site VPN clients as an access method.

(c) Client-owned Privileged Access Management (PAM) or Identity Access Management (IAM) platforms.

Any access methods outside of those listed in this section will be subject to NTT approval and may be subject to additional charges.

4.4 Privileged User Access (Admin Rights)

NTT will deploy and configure servers and devices with the users and associated level of Admin Rights required to provide the Service. NTT will use its standard Privileged Access Management (PAM) and Identity Access Management (IAM) platforms to manage access within the Client environment. NTT will be the only party having Admin Rights on all items under management. No shared management models are accepted by default without the Shared Management Model rider or Risk exception executed by the Client.

(a) Management Tools

The configuration and placement of NTT's management tools are dependent upon solution requirements. The following guidelines generally apply:

(i) For platforms consisting of thirty (30) or more managed devices, NTT will require dedicated management tools, which can be hosted within the Client's infrastructure or within a dedicated management zone.

(ii) For platforms consisting of fewer than thirty (30) managed devices NTT may use shared management tools but subject to the following restrictions:

For full stack platforms (systems and networking) shared management tools require no destination NAT between NTT and the Client platform; the use of NAT will require certain tools such as monitor collectors to reside within the Client's infrastructure, on a dedicated server.

Networking-only platforms carry no NAT restrictions:

Bidirectional connectivity is required for some management tools and must be considered when NAT is used:

(iii) For platforms with PCI compliance requirements, dedicated tools are required regardless of platform size.

(iv) Ticketing and monitoring are delivered with NTT's own toolsets.

(v) Certain managed services may require the installation of additional agents and tools.

(vi) Knowledge Management content will be stored in NTT's current tool.

4.5 Services Portal

NTT will deliver a single view of the Client's entire technology estate, regardless of the locations in which physical and logical assets are based, using its Services Portal. The Services Portal shall provide:

(a) A secure browser accessible platform

(b) Ability to apply role-based access and permission to portal users

(c) Access to NTT support team via ticketing system

(d) Tracking of Incidents and Incident resolution

(e) Visibility of CMDB items

(f) Event monitoring, alerting and performance monitoring

(g) Monitoring of managed services activities (changes, patching, compliance)

(h) One consolidated view for all the platforms and solutions managed by NTT

The service portal may be updated by NTT in its discretion.

4.6 NTT ITSM and CMDB

NTT will solely use its own ITSM platform which has been developed to support the business and operations of its Managed Services.

4.7 Monitoring

Monitoring is a function of the Service, and NTT uses several tools, each one specifically selected for the task.

Note: Only monitoring tools proposed by NTT will be valid for measuring the performance and the availability of the Client solution. Should the Client wish to use their own monitoring tools in addition to those provided by NTT, the following restrictions apply:

(a) The Client tool must coexist with the NTT tools, but it will not replace them

(b) Event integration with Client monitoring tools is out of scope

(c) For purposes of providing the Service, only the monitoring tools provided by NTT will be considered the "source of truth" for Event and performance data

(d) In the event of performance issues caused by Client monitoring tools, NTT will request that the Client disable their monitoring. Should the Client refuse, NTT will suspend its SLA until the problem is resolved.

5 Service Delivery Roles & Responsibility

5.1 Integrated Operations Center

The Integrated Operations Center (IOC) is the primary point-of-contact for the Client. Clients can make service requests, report Incidents, and check on tickets via phone and/or email. The IOC maintains total ticket ownership and is staffed with both IT support analysts and application support specialists so that no additional call routing is necessary.

The IOC is primarily responsible for:

(a) 24 x 7 x 365 Interaction handling with end-users (Ticket, Mail, Chat, and Phone)

(b) 24 x 7 x 365 Response to monitoring alerts

(c) 24 x 7 x 365 Basic Incident Management

(d) 24 x 7 x 365 Basic Service Request fulfillment

5.2 L2-L4 Engineering

NTT delivers L2-L4 support with our technical team “pod” strategy. Within these pods, all the technical resources assigned to provide managed services are structured into dedicated teams and assigned to the Client to provide a cohesive support model.