NTT DATA

Service Description: SBCaaS

This document, including any referenced materials expressly incorporated herein ('**Service Description**'), describes in general the features and functions of (and associated obligations, limitations, and conditions relating to) NTT DATA's SBC-as-a-Service (SBCaaS) (the '**Services**') from NTT DATA's Managed Employee Experience (MEX) service portfolio.

This Service Description is maintained by NTT DATA at this URL (or successor site) and may be updated by NTT DATA from time-to-time (effective upon publication).

Part A. Service Overview

General Description

1.1   NTT DATA's SBCaaS offers a cloud-based service, centrally managed by NTT DATA, that enables rapid deployment of a virtual SBC and gives the Client access to service management tools, security features, and systems for controlling associated traffic flow.

Carrier Circuit Coordination

1.2   As a component of SBCaaS, NTT DATA will monitor the interface of Client's third-party contracted "bring your own carrier voice" circuit terminating on an interface managed by NTT DATA, and:

(a)   record, log, and manage the availability of the interface; and

(b)   work to resolve issues on behalf of the Client with the third-party carrier for the contracted carrier voice circuit.

1.3   Client acknowledges the Carrier Circuit Coordination services only apply to the interface of Client's third-party contracted "bring your own carrier voice" circuit under the management of NTT DATA and that NTT DATA does not monitor, nor is NTT DATA responsible for, internet availability.

1.4   NTT DATA's provision of the Carrier Circuit Coordination add-on service component is contingent on Client providing NTT DATA with a letter of authorization (LOA) authorizing NTT DATA to act as Client's agent for the purpose of addressing relevant Incidents with the applicable third-party carrier. Client will notify its third-party carrier that such authorization has been granted to NTT DATA for Client contracted carrier voice circuits.

Part B. Transition-In Period

1   Description

1.1   In relation to the Services, transition refers to the process of moving Client's collaboration environment to be under the management and responsibility of NTT DATA or, as applicable, otherwise enabling activation of the relevant Services, as scoped in the SOW and subject to all applicable terms and conditions of the Agreement.

2   Project coordination

2.1   The overall management of the entire transition project is facilitated through the transition manager, appointed by NTT DATA and a joint steering committee with designated representatives from both parties, if required. If implemented, the steering committee will make all executive level decisions regarding the direction of the project and resolve any major conflicts or concerns presented by the transition manager.

2.2   During the transition period an established process will be followed, which will be coordinated and managed by designated representatives from both parties. These parties must make themselves available to assist and provide input into the execution of the process.

3   Client obligations

3.1   In respect of the Services, Client must transfer management responsibilities of the Configuration Items to NTT DATA, prior to the migration and deployment.

3.2   On NTT DATA's reasonable request, Client must supply NTT DATA with specific information to enable provision of the Services, including but not limited to:

(a)   information about Client, Configuration Items (and associated Users), and associated attributes, access methods and any other relevant technical information;

(b)   authorized contacts who can log Incidents and Service Requests;

(c)   Client contacts for priority escalation purposes;

(d)   relevant processes and policies; and

(e)   contact information for third-party supplied equipment, services or maintenance and service support of such equipment or services.

4   Service Portal configuration and access

4.1   Where applicable NTT DATA will, during the Transition-In Period:

(a)   create and configure a Service Portal for Client

(b)   provide access to end-users as identified by Client; and

(c)   provide Client with instructions for navigating the Service Portal.

5   User acceptance testing

5.1   NTT DATA will commence delivery of the steady-state Services following a successful user acceptance testing process, as determined based on the criteria defined by NTT DATA during transition and, upon completion thereof, confirmed by Client (with such confirmation not to be unreasonably withheld).

Part C. Service Features

In relation to the steady-state Services, the complete list of Service Features and the parties' respective rights and obligations in respect thereof are as follows:

1   Case management

Tier 2 Case management

1.1   NTT DATA will raise an Incident record as a result of:

(a)   Client logging a Case with NTT DATA through the Service Desk;

(b)   Client logging a Case with NTT DATA via the Services Portal; or

(c)   detection of an Event on monitored Configuration Items.

1.2   Following the creation of the Case, a related Incident record will be created, and NTT DATA will respond to Client to confirm the initial Case classification and prioritization.

1.3   Client must:

(a)   raise Priority 1 and 2 Cases with the Service Desk by telephone only; and

(b)   provide NTT DATA with Client contacts authorized to log Cases and notify NTT DATA of any changes to these contacts.

1.4   Client may request the escalation of a Case to a higher Priority level by contacting an escalation manager through the Service Desk and quoting the Case reference number.

1.5   NTT DATA may downgrade an escalated Case if it is being managed to a scheduled timeframe, or resolution has been provided to Client and is in the process of being tested.

1.6   Where Client initiated the escalation, NTT DATA will obtain Client's approval prior to downgrading.

Tier 2 Incident Diagnosis and Resolution

1.7   NTT DATA will:

(a)   remotely diagnose the cause of the Incident by connecting to the supported Configuration Item to perform Incident diagnosis; or

(b)   remotely diagnose the cause of the Incident within any Manufacturer or Third-Party Supplier cloud environment or user diagnosis, by connecting to the relevant administration consoles to validate / perform diagnosis;

(c)   suggest a course of action to resolve the Incident or put a Workaround in place; and

(d)   update Client on progress.

1.8   Once the Incident is resolved, NTT DATA will:

(a)   close the Incident record; and update the Case; or

(b)   notify Client of resolution and closure of the Case record.

1.9   Where an Incident is caused by Client making changes to Configuration Items, Client may incur an additional charge.

1.10 Where an Incident is identified as a potential product defect, NTT DATA will engage with Client's third-party maintenance provider and coordinate activities on behalf of Client until the Incident is resolved. To facilitate the above, Client will provide NTT DATA with a letter of authorization (LOA) authorizing NTT DATA to act as Client's agent for the purpose of addressing relevant Incidents. Client will notify its third-party maintenance provider that such authorization has been granted to NTT DATA for the applicable items within the Configuration Item list.

1.11 An Incident may be classified as a Major Incident, where NTT DATA agrees that specific criteria are met, including:

(a)   there is no availability of an application workload resulting in the Services not being available (i.e., no calling, one-way audio, no meeting) which impacts the following:

(i)   entire site impacted / several groups of Users >= 50% of the active User population;

(ii) scale: group of several Users >= 20% of the active User population

1.12 NTT DATA will channel a Major Incident through a stricter resolution process that includes, where possible:

(a) shorter timeframes.

(b) assignment of additional resources; and

(c) assignment of a dedicated Major Incident manager.

Incident Reporting

1.13 NTT DATA will provide Client with Incident management reporting information, including:

(a) statistical information in respect of Incident management; and

(b) Incident management Service Level Target achievement.

2 Event management

Event handling

2.1 NTT DATA will:

(a) monitor for Events for the supported Configuration Item's within the agreed Service Calendar;

(b) assess Events against predefined rules;

(c) where possible, resolve Events automatically; or

(d) route Events according to the relevant process for investigation and resolution.

Event optimization

2.2 NTT DATA will, periodically:

(a) identify opportunities to optimize Event handling; and

(b) where possible, add new automation rules to the Service Management System.

3 Service asset and configuration management

Configuration Item identification and recording

3.1 NTT DATA will:

(a) record pre-defined Configuration Items, as set out in the SOW; and

(b) provide Client with access to this information.

Vendor update notification

3.2 NTT DATA will provide Client with relevant vendor notification information, including:

(a) patches;

(b) end-of-X milestones;

(c) minor feature releases; and

(d) Security Vulnerabilities.

3.3 NTT DATA can notify Client in terms of clause 3.2 above only in the event that it receives the notification from the relevant Manufacturer. Accordingly, and for the avoidance of doubt, where the Manufacturer does not provide notifications in respect of a Configuration Item (for example that the Configuration Item has reached End-of-Life), NTT DATA will not be liable for performance of this Service Feature.

Configuration Item control and updates

3.4 Where, in NTT DATA's performance of the Services, a Configuration Item's attributes are altered, NTT DATA will update the attributes accordingly.

3.5 Where Client makes changes to a Configuration Item attribute, Client must promptly notify NTT DATA by logging a Case.

Configuration Item Data

3.6 NTT DATA will:

(a) use NTT DATA and/or Manufacturer data sets to enrich Client-provided Configuration Item data with additional, applicable information; and

(b) have exclusive write access to all Configuration Items covered by the Services.

3.7 In addition to any other Client responsibilities set out in the Agreement, including as specified in the SOW, Client must, no less than 5 business days prior to the agreed scheduled discovery activity, notify its operational and security teams, as applicable, and implement appropriate change controls to avoid "false positive" security alerts.

4 Change management

Change Request management

4.1 NTT DATA will raise a Change Request record

 (a) as a result of Client logging a Case relating to Change Request with NTT DATA through the Service Desk;

 (b) as a result of Client logging a Case relating to Change Request with NTT DATA via the Services Portal; or

 (c) as part of the performance of its obligations under a Deliverable.

4.2 Following the creation of a Change Request record, NTT DATA will respond to Client to confirm the initial Change Request classification via a Case.

4.3 NTT DATA will manage the lifecycle of a Change Request in accordance with the Change Request classification.

4.4 Change management is not included for any WAN circuit(s) that are included in the Configuration Item list. Client must inform NTT DATA of any service changes that are implemented on a WAN circuit by their third-party carrier service provider, which may require a Service Request to change a Configuration Item upon which the WAN circuit terminates.

Change impact analysis

4.5 Based on the information available, NTT DATA will assess and determine the impact of a Change Request on:

 (a) the Configuration Item(s); and

 (b) the forward schedule of changes, as advised by Client.

4.6 NTT DATA will make the results of the change impact analysis available to Client.

Change planning

4.7 NTT DATA will produce a plan, as suited and appropriated for the type of change being undertaken, to streamline the change management process ('**Change Plan**'), with input from Client, for Change Requests, that includes:

 (a) identification of any products required;

 (b) where possible, a test plan for testing the change prior to roll-out;

 (c) tasks for the implementation of the change;

 (d) determination of the number and availability of NTT DATA and Client representatives required to implement the change;

 (e) identification of any additional ongoing resources required once the change is implemented;

 (f) a plan for the roll-back of a failed or failing change;

 (g) calculation of the time required to implement the change; and

 (h) time and material quotation to implement the change.

4.8 NTT DATA will submit the Change Plan to Client for approval and for submission to the Change Advisory Board, if applicable.

Change implementation

4.9 NTT DATA will, upon receipt of approval from Client to proceed, implement the Change Request according to the approved Change Plan, as agreed with Client:

 (a) on a time and materials basis at an additional charge;

 (b) through remote fulfilment of Service Requests, where applicable, and as per process set out in section 5 of this Service Description; or

 (c) through a formal consulting and professional services engagement, the scope and pricing of which will be agreed with Client and set out in a separate statement of work.

4.10 NTT DATA will implement changes to Configuration Items in alignment with the agreed change management process, as notified by Client and agreed to by NTT DATA, to the extent practicable, only following the testing of such changes by NTT DATA in a non-production environment of the Client or tested on a live Configuration Item agreed by the Client at the Client's risk.

Change reporting

4.11 NTT DATA will provide Client with change management reporting information, including statistical information in respect of change management.

5 Request fulfillment

Service Request management

5.1 NTT DATA will raise a Service Request as a result of:

 (a) Client logging a Case relating to a Service Request with NTT DATA through the Service Desk.

(b)   Client logging a Case relating to a Service Request with NTT DATA via the Services Portal; or

(c)   where made available by NTT DATA, Client completing a self-service Service Request via the unified provisioning application within the Services Portal.

5.2   Following the creation of a Service Request record, NTT DATA will respond to Client to confirm the initial Service Request classification and prioritization via the Case reference number.

5.3   Client may request the escalation of a Service Request to a higher Priority level by contacting an escalation manager through the Service Desk and quoting the Case reference number.

5.4   NTT DATA may downgrade an escalated Service Request if it is being managed to a scheduled timeframe, or where a resolution has been provided to Client and is in the process of being tested.

5.5   Where Client initiated the escalation, NTT DATA will obtain Client's approval prior to downgrading.

5.6   Client must log Priority Service Requests with the Service Desk by telephone or via the Services Portal with a follow up telephone call.

5.7   Service Request management is not included for any WAN circuit(s) that are included in the Configuration Item list. Client must inform NTT DATA of any service changes that are implemented on a WAN circuit by their third-party carrier service provider, which may require a Service Request to change a Configuration Item upon which the WAN circuit terminates.

Service Request fulfilment

5.8   A Service Request is a Standard Change, which is requested via Case management within the Services Portal, with pre-defined Service Request Fulfilment catalogue details, which:

(a)   is pre-approved by Client;

(b)   relates directly to a Configuration Item;

(c)   can be performed remotely using the site-to-site connection;

(d)   is executable by a vendor-certified engineer;

(e)   requires no scoping or project management for its completion; hould not as a single task take more than 2 hours to perform;

(f)   when performed as part of a set of requested tasks (i.e., repeating the same single instance or similar tasks in multiple locations or for multiple Configuration Items) does not take more than 4 hours to perform; and

(g)   has a set of procedures or work instructions available to complete.

5.9   Where a Service Request is raised:

(a)   the Service Request is considered pre-approved by Client;

(b)   NTT DATA will schedule the implementation of the Service Request as agreed with Client;

(c)   should the Service Request as a single task take more than 2 hours to perform or include multiple tasks that exceed 4 hours of effort, NTT DATA will perform the work, as agreed with Client:

(i)   on a time and materials basis at an additional charge; or

(ii)   through a formal consulting and professional services engagement, the scope and pricing of which will be set out in a separate statement of work.

5.10   Subject to the Fair Usage Policy and associated terms (as described further in Part A, clause 8 of the Specific Term), NTT DATA will fulfil the Service Request through utilizing Service Units associated to each Client Case raised for Service Request Fulfilment types, as categorized within the Services Portal

5.11   For the avoidance of doubt, Client will remain responsible for the mitigation of any risks associated with the implementation of the Service Request and ensure changes are internally approved and communicated.

Requests for information fulfilment

5.12   Where Client raises a Case for a Service Request for information in respect of a procured Service, NTT DATA will use commercially reasonable efforts to collate the required information and supply it to Client at no additional charge.

5.13   Where Client raises a Case for a Service Request for information that is neither in respect of a procured Service nor executable with commercially reasonable efforts, NTT DATA reserves the right to fulfil the request for information on a time and materials basis at an additional charge.

Service Request reporting

5.14   NTT DATA will provide Client with Service Request reporting information on a monthly basis, via the Services Portal including:

(a)   statistical information in respect of Service Requests;

(b)   information in respect of Service Unit usage; and

6   Release and deployment management

Technology updates and minor releases

6.1   Technology updates or patches means software updates comprised of code inserted or patched into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package.

6.2   Minor releases (software updates and dot releases) are also known as maintenance releases. They include corrections, extensions, or fixes to an existing full release.

6.3   NTT DATA will implement minor feature releases in relation to Security Vulnerabilities for technology updates where made available by the specific Manufacturer. Any additional support will be subject to additional charges on a time and materials basis.

Release and deployment recommendations

6.4   NTT DATA will make recommendations in respect of the relevant Manufacturer notifications, including:

 (a)   recommended actions to be taken (which could include the recommendation to conduct a more detailed investigation); and

 (b)   where possible, the estimated cost of the remediation or recommendation by NTT DATA.

Release and Deployment Planning

6.5   NTT DATA will conduct release package planning and preparation that includes:

 (a)   definition of the release package scope;

 (b)   performance of a risk assessment;

 (c)   identification of roles/responsibilities to deploy the release package;

 (d)   where possible, a test plan for testing the release package prior to roll-out;

 (e)   definition of the pass/fail criteria;

 (f)   deployment schedule; and

 (g)   a plan for the roll-back of a failed or failing release package deployment.

6.6   Based on the above, NTT DATA will develop and submit a release and deployment plan to Client for approval.

Release package building and testing

6.7   NTT DATA will:

 (a)   build, deploy and, where possible, test the release package on low-risk Configuration Items or other assets in Client's environment as agreed with Client and documented in the release and deployment plan; and

 (b)   on completion of release package testing, update and submit a release and deployment plan to Client for approval to proceed to deployment.

Release package deployment

6.8   NTT DATA will, upon Client's approval to proceed, deploy the release package according to the approved release and deployment plan.

6.9   For the avoidance of doubt, NTT DATA is not responsible for the functionality and applicability of a Manufacturer-provided release package.

Release and deployment reporting

6.10   NTT DATA will, periodically, provide Client with release and deployment reporting information, including:

 (a)   statistical information in respect of release and deployment; and

 (b)   number of release and deployment requests.

Early Life Support

6.11   NTT DATA will resolve any initial Incidents and Problems associated with the release package within an early life support period of 5 business days from deployment and on a reasonable commercial effort's basis.

7   Service level management

Service level monitoring and reporting

7.1   NTT DATA will monitor its performance against the Service Level Targets agreed with Client and will make monthly service management information available to Client via the Services Portal.

7.2   The service level information does not include reporting on any service levels objectives agreed between Client and a third party, including any Third-Party Supplier.

7.3   NTT DATA may, on written request by Client, agree to produce customized or additional reporting at an additional charge.

8   IT security management

Security policy implementation

8.1   NTT DATA implements and manages Configuration Items to its applicable certified ISO standards.

8.2   NTT DATA will, subject to clause 8.3 below, implement and maintain security controls in accordance with NTT DATA's standard security policies, as applicable to the Services.

8.3   Client must align to NTT DATA's standard security policies applicable to the Services before NTT DATA's commencement of the Services. Any Client security policies that are not aligned (or subsequently become unaligned) to NTT DATA's standard security policies must be notified to NTT DATA with reasonable written notice for NTT DATA to review and determined whether it can accommodate Client's security policy, provided that:

(a)   NTT DATA will not be obligated to comply with any Client security policy that is not technically or commercially feasible; or materially impairs NTT DATA's ability to provide the Services as contracted under the applicable SOW; and

(b)   NTT DATA may make a corresponding adjustment to the Charges for the Services for any changes to Client security policies which result in NTT DATA incurring additional costs or expenses.

9   Technical management

Standard operating procedure (SOP) development and maintenance

9.1   NTT DATA will, in consultation with Client, identify, develop, and maintain standard operating procedures required for the Services in accordance with agreed technology standards.

9.2   Standard operating procedures shall include:

(a)   troubleshooting procedures to manage Events and resolve Incidents;

(b)   Client equipment and operating system standard configurations; and

(c)   system(s) administration guide(s).

10   Service Delivery Manager

10.1   NTT DATA will assign a service delivery manager to Client. This function will be provided as a shared resource and the in-scope activities, as described below, will be performed remotely. Activities not listed below will be out of scope for this Service Feature. The activities of the service delivery manager will include:

(a)   acting as a primary point of contact for Client in respect of Services delivery escalations and support;

(b)   bringing key issues and applicable recommendations identified in the course of delivering the Services to the attention of Client in relation to Manufacturer notifications, Change Requests and release and deployment activities.

(c)   interactions with the Client for processes such as service asset configuration management (SACM) updates following change management and additional activations of Configuration Items within the CMDB inventory;

(d)   providing service level governance and reporting as agreed on a monthly basis either remotely or in person, as aligned to the agreed service location and resource alignment;

(e)   capture, track and manage contractual issues and escalations in the Services Portal, in accordance with agreed escalation governance paths; and

(f)   co-ordinate with Client for services outside of the scope listed within the SOW to quote on a time & materials basis.

Part D. Services Portal

1   Services Portal description

1.1   NTT DATA will deliver a single view of the collaboration environment under management, regardless of the locations in which physical and logical assets are based, using its Services Portal. The Services Portal can be used by Client as an interface to interact with NTT DATA, monitor the state of the solution, and view the list of contracted Services.

2   Services Portal attributes

2.1   The primary attributes of the Services Portal are as follows:

(a)   a secure browser accessible platform, available 24 x 7 x 365;

(b)   ability to apply role-based access and permission to portal users on specific systems;

(c)   access to NTT DATA support team via ticketing system; and

(d)   visibility of the configuration management database (CMDB).

Sensitivity Label: General