

## Specific Terms: NTT DATA Managed M365 Collaboration

The service-specific terms and conditions set out in this document ('**Specific Terms**') are incorporated in and apply to the SOW formed between NTT DATA and Client for the provision of NTT DATA's Managed M365 services and, as well as the optional add-on service components made available by NTT DATA in connection therewith (the '**Services**').

Unless otherwise specified therein, the Specific Terms set out in Part A apply to all Managed M365 Services, including any add-on service components purchased by Client and included within the scope of the relevant Managed M365 SOW.

The Specific Terms set out in Part B supplemental to Part A and only apply to the specific optional add-on service component indicated therein (to the extent such add-on service component is purchased by Client and included within the scope of the relevant Managed M365 SOW).

These Specific Terms are 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. Managed M365 Collaboration Services

---

#### 1 Service-specific definitions

1.1 Capitalized terms used but not defined in these Specific Terms will have the same meaning otherwise set out in the Agreement.

1.2 As additional or amended defined terms in these Specific Terms (or as used in the applicable SOW):

**Availability** means the ability of an IT service or other Configuration Item to perform its agreed function when required.

**Business Day** means Monday through Friday from 9 a.m. to 5 p.m. local time and excludes weekends and public holidays.

**Case** means Client-related cases created within the NTT DATA Services Portal that are a mechanism for capturing the details of a service, project, transaction, or response to Client requests for management of any Incident, Service Request or Change.

**Change Advisory Board (or CAB)** means a formalized body that supports the assessment, prioritization, authorization, and scheduling of changes and comprises Client and, if applicable, NTT representatives.

**Change Request** means a request generated by Client or NTT for the addition, modification, or removal of anything that could have a material impact on a Configuration Item or the provision of the Managed M365 Services and any Service Feature thereunder.

**Client Connectivity and Prerequisites Guide** mean the document that describes the mechanics on what is required technically to be configured within Client's collaboration environment to enable access and protocols to deliver the Managed M365 Services.

**Configuration Item** means any Room or User supported as part of the Managed M365 Services.

**End-of-Life** means the relevant Configuration Item is no longer manufactured or supported, as determined by NTT DATA, based on any end-of-life or end-of-service announcements made by the Manufacturer.

**Event** means a change of state that has significance for the management of a Configuration Item.

**Incident** means, in relation to Managed M365 Services, an unplanned interruption or reduction in quality related to one or more supported Configuration Items.

**Major Incident** means an Incident that meets specific criteria and has a high severity impact on Client or for which NTT DATA warrants a greater organizational focus to manage.

**Manufacturer** means either the original equipment manufacturer of any relevant hardware or the owner or licensor of any relevant software, as applicable.

**Permanent Resolution** means the action taken to resolve the root cause of an Incident or a Problem.

**Priority** means the relative urgency and importance of an Event, Incident, Problem, Change Request, or Service Request, based on a combination of impact and urgency, with Priority 1 being the highest and Priority 5 being the lowest.

**Privileged Access Management (or PAM)** means the application used by NTT DATA support engineers to securely access Client's in-scope tenant applications in order to deliver the Managed M365 Services, as described further in clause 6.8 below.

**Problem** means the cause of one or more Incidents.

**Security Vulnerabilities** means an unintended flaw in software code or a system that leaves it open to the potential for exploitation in the form of unauthorized access or malicious behavior such as viruses, worms, Trojan horses and other forms of malware.

**Service Calendar** means the hours specified in the SOW during which NTT must perform its obligations under a Service Feature in respect of a Configuration Item.

**Service Commencement Date** means the date of Service Acceptance for the steady-state Managed M365 Services, as described in clause 2.1 below.

**Service Desk** means the NTT DATA service desk that acts as a single point of contact between NTT DATA and Client to manage all Incidents, Problems, Change Requests and Service Requests, and all related communications and escalations with Client.

**Service Feature** means, with respect specifically to the Managed M365 Services delivered pursuant to these Specific Terms, a specific feature or outcome of the Services, as identified in the applicable Service Description.

**Service Level Target** mean the service commitments set out in the Service Levels.

**Service Management System** means the system used by NTT DATA to record information relating to the supply of the applicable Managed M365 Services.

**Service Operations Manual** means a reference document provided to Client (prior to the Service Commencement Date), which describes how to contact and interact with NTT DATA in connection with the Managed M365 Services being delivered.

**Service Request Catalogue** means a list of approved requests within a catalogue, that are generated by Client or NTT DATA for information, for a Standard Change, or for access to a service or report, and that is managed by the Service Request Fulfilment process.

**Service Request Fulfilment** means the process responsible for managing the lifecycle in respect of a Service Request generated by Client or NTT DATA.

**Service Unit** means a unit of measure that is used to track and calculate specific Service Request Fulfilment activities on a consumption basis, as set out in the Service Request Catalogue.

**Services Portal** means the internet portal created and configured by NTT DATA for access by Client as part of the Managed M365 Service.

**Standard Change** means a low risk, relatively common change that is mutually agreed and documented and constitutes a preapproved change that is implemented through a Service Request.

**Third-Party Supplier** means a third-party company or entity with whom Client will have a separate agreement to provide a product or a service to maintain a Configuration Item at an operational level. This may include an Affiliate of NTT DATA, provided that in such a case, the relevant product or service would remain subject to a separate Order or SOW with such Affiliate of NTT DATA.

**Unified Monitoring Application (or UMA)** means the connectivity, infrastructure, and applications delivered by NTT DATA to monitor Client's Configurations Items to trigger alerts, indicate health status, and display reporting in the Services Portal.

**Unified Provisioning Application (or UPA)** means the connectivity, infrastructure, and applications delivered by NTT DATA to perform self-service MACDs on Client's Configurations Items from the Services Portal.

**Workaround** means a set of actions that reduces or eliminates the impact of an Incident or Problem for which a Permanent Resolution is not yet available.

## 2 Scope of Services

### Service commencement

2.1 The provision of steady-state Managed M365 Services, as set forth in the relevant SOW, will commence on the Service Commencement Date and, unless terminated earlier in accordance with the terms of the Agreement, will endure for the SOW Term. The Service Commencement Date will be declared upon the earlier to occur of:

- (a) the first production or non-test Configuration Item being onboarded to the steady-state Managed M365 Services; or
- (b) receipt of Client's written confirmation (via email) that the following service acceptance criteria for the steady-state Managed M365 Services has been met:
  - (i) the in-scope managed service components for the Managed M365 Services have been enabled and made available to Client.
  - (ii) Client has received and approved the Service Operations Manual; and
  - (iii) Client has verified completion of any service acceptance testing, as set out in the relevant transition plan or otherwise previously agreed by the parties.

with the applicable milestone, as set forth in (a) and (b) above, being deemed '**Service Acceptance**'. If neither (a) nor (b) above have occurred within 10 days from NTT DATA giving Client notice that the relevant service acceptance criteria has been met, Service Acceptance will be deemed to have occurred on the day immediately following the expiration of such 10-day notice period.

### Service Features and scope

2.2 The Managed M365 Services consist solely of the Service Features which, together with the parties' respective obligations thereunder, are set out in the applicable Service Description and NTT DATA will only supply to Client those Service Features in respect of the Configuration Items specifically set out in the SOW..

- 2.3 Technology that is not supported as a standard supported technology by the Managed M365 Services must be approved by NTT DATA before it is included in scope of the Managed M365 Services.
- 2.4 Where there are variations to a Service Feature that are specific to a given Managed M365 Service, or where there is provision made for Service Features to be customized as part of a given Managed M365 Service, such varied or customized Service Features, and the parties' respective obligations thereunder, will be set out in the applicable SOW.

### 3 Location of Services

- 3.1 NTT DATA will provide the Managed M365 Services from its service management locations, as may be set out in the applicable SOW or otherwise determined by NTT DATA.
- 3.2 Clause 3.1 notwithstanding, the service management and public or private cloud infrastructure locations relating to any third-party platforms or services provided by Third-Party Suppliers (including any public or private cloud environments) are solely determined by the applicable Third-Party Supplier or as may be selected by Client based on the options made available by such Third-Party Supplier. Client acknowledges and accepts that any such Third-Party Suppliers are solely responsible for the provision of any relevant third-party platforms and services, including, as applicable, any data transfer or residency policies and failover or disaster recovery services connected therewith.

### 4 Service Management System

- 4.1 NTT DATA may, in relation to the Managed M365 Services delivered pursuant to these Specific Terms, make adjustments or add enhancements to its Service Management System during the SOW Term. NTT DATA will provide advance notice of any such changes, where possible.

### 5 Configuration Items

- 5.1 The applicable SOW will set out the Configuration Items, identifying the relevant Devices and User licenses and corresponding details. The Device and User license lists will be subject to change on an ongoing basis as Devices and User licenses are changed, added, and removed in accordance with NTT DATA processes. At any point in time, the definitive list of Configuration Items under management will be as specified in NTT DATA's Service Management System.
- 5.2 Where NTT DATA determines that it is unable to continue to provide the Managed M365 Services on an End-of-Life Configuration Item, NTT DATA may, by giving Client at least 90 days' prior written notice, remove the End-of-Life Configuration Item from the Device or User license list, as applicable.
- 5.3 In addition to the Client obligations described in these Specific Terms and any general obligations set out in the Agreement (including as may be specified in the SOW), Client must:
- (a) complete any transition tasks and changes to Configuration Items, as set out in the SOW or otherwise reasonably requested by NTT DATA, to enable the provision of Managed M365 Services and allow NTT DATA to perform its obligations thereunder;
  - (b) ensure that Configuration Items are covered by valid hardware and software maintenance contracts, with service levels and response times that align with the Service Level Targets and response times to be provided by NTT DATA;
  - (c) keep all records relating to use and performance of the Configuration Items as NTT DATA may reasonably request and ensure that NTT DATA personnel have access to such records at all reasonable times;
  - (d) keep an up-to-date copy of configuration files or other relevant information for all Configuration Items and provide a copy to NTT DATA when requested, except where NTT DATA is responsible for this as part of its contractual obligations to Client under a Service Feature;
  - (e) maintain backups of configuration files (which NTT DATA will work with Client to restore in-scope Configuration Items, if needed);
  - (f) notify NTT DATA through a Service Request of all changes to configuration files, including User access credentials, that will affect Configuration Items and the configuration download, no less than 2 business days before implementing the change;
  - (g) maintain the integrity of log files associated with a Configuration Item to enable NTT DATA to fulfil its diagnostic obligations. In the event log files are deleted or modified, Client will incur an additional charge for NTT DATA to remediate;
  - (h) review and validate the information stored in the Device and User license lists, as applicable, and notify NTT DATA of any discrepancies on a regular basis; and
  - (i) ensure the correct software versions are installed on all Devices to enable NTT DATA to retrieve configuration files.

### 6 Client obligations

#### Client equipment, network, and systems

- 6.1 Client must ensure that any of its equipment, network, or systems connected to any NTT DATA equipment, network, or systems used in receiving the Managed M365 Services is technically compatible, connected, and used in accordance with any instructions or safety and security procedures, as communicated by NTT DATA.
- 6.2 If any Client equipment, network, or systems do not comply with the requirements of clause 6.1 above, Client must promptly advise NTT DATA. Upon notice from NTT DATA, Client must disconnect such equipment, network, or systems, or, where applicable, permit NTT DATA to do the same, the cost of which will be borne by Client.
- 6.3 NTT DATA makes no warranty regarding the interoperability between the NTT equipment, network, or systems and any Client equipment, network, or systems.

**User applications and software**

- 6.4 Client must ensure that all User workstations accessing the functionality or receiving the benefit of the Managed M365 Services have supported and compatible versions of the necessary User applications and software, including web browsers and operating systems, installed and maintained during the SOW Term.

**Licensing**

- 6.5 Unless the applicable SOW expressly indicates that NTT DATA will procure specified third-party licenses for or on behalf of Client in connection with the Managed M365 Services, Client must procure and maintain all relevant third-party licenses from any Third-Party Supplier necessary for Client's use of the Managed M365 Services.
- 6.6 Without limiting Client's obligations under clause 6.5 above, for the vendor platform deployment model, Client must adhere to all applicable license mobility requirements for any Client-provided licenses procured from a Third-Party Supplier, including without limitation the timely submission of any license verifications forms.

**Client connectivity**

- 6.7 In order to enable NTT DATA to provide the Managed M365 Services in accordance with the applicable SOW, Client will comply with all requirements specified in the Client Connectivity and Prerequisites Guide and will perform all Client obligations specified therein, including but not limited to providing NTT DATA with access via routing and firewall rules to all IP addresses that NTT DATA is required to manage under the applicable SOW. Where this is the required, NTT DATA will provide all IP address ranges needed to configure conditional access controls.

**Privileged Access Management (PAM)**

- 6.8 In order to enable NTT DATA to provide the Managed M365 Services in accordance with the applicable SOW, Client must permit NTT DATA to enable one of the supported Privileged Access Management (PAM) options, as detailed further in the Client Connectivity and Prerequisites Guide. Client must inform NTT DATA of its preferred PAM option prior to the start of transition activities, and depending on the elected option, additional one-time fees and recurring monthly Charges may apply.

**Client Microsoft Active Directory**

- 6.9 Client will ensure that its Microsoft Active Directory configuration, including the forest level, service packs, and patches, are compatible with the Managed M365 Services.

**Third-Party platform access requirements**

- 6.10 In order for NTT DATA to enable Client to have the ability to self-provision, automate (where required by the Client), manage voice users, perform extension number management and voice policies, etc. within their collaboration environment using the Services Portal, Unified Provisioning Application (UPA), and Unified Monitoring Application (UMA), Client must provide a level of access to either their Microsoft Azure Active Directory and Microsoft Teams platform, or to their Cisco Webex Control Hub for the synchronization and execution of such tasks. The Client Connectivity and Prerequisites Guide details these technical requirements in-depth and NTT DATA will review these requirements with the Client in advance of the onboarding of the Managed M365 Services to ensure all Client security policies and requirements are adhered to wherever possible.

**Change management**

- 6.11 Client acknowledges that the change management service feature (as described in the Managed M365 Service Description) is not generally subject to co-management between Client and NTT DATA and accordingly Client may not perform its own Service Request Fulfilment except for any Service Request Fulfilment task expressly identified as a self-service MACD in the Service Request Catalogue (which may be performed by the Client's administrator via the Services Portal).

**7 Maintenance**

- 7.1 From time-to-time NTT DATA will schedule preventative maintenance (**Scheduled Maintenance**) for the Managed M365 Services which may lead to non-achievement of Service Level Targets. Wherever possible, Client will be given no less than 14 days prior notice of the Scheduled Maintenance and the Scheduled Maintenance will occur within the maintenance window specified in the table below:

Day	Scheduled Maintenance window
Monday – Saturday	12h00 am - 06h00 am
Sundays	12h00 am - 08h00 am

For purposes of the timing specified in the table above, the Client’s local time zone where the Scheduled Maintenance is to be performed is applicable.

7.2 Scheduled Maintenance may be attributable to, inter alia:

- (a) preventative maintenance;
- (b) system moves or reconfigurations;
- (c) system testing of new systems or enhancements;
- (d) upgrades, application of security patches, application patches;
- (e) operating system patches; and
- (f) implementations of new systems or enhancements.

7.3 NTT DATA may also be required from time to time to conduct unscheduled maintenance (**‘Unscheduled Maintenance’**) for the Services, attributable to factors outside of its reasonable control, including but not limited to the service level exclusion events specified in clause 3 of the Service Levels, which may lead to non-achievement of Service Levels Targets. In such circumstances NTT DATA will endeavor to provide Client with as much prior notice of such Unscheduled Maintenance as is reasonable under the circumstances.

8 Fair Use Policy

8.1 NTT DATA will not charge Client for individual in-scope Service Requests. NTT DATA employs a ‘fair use’ policy under which NTT DATA reserves the right to limit the number of in-scope Service Requests after an extended timeframe where Client has initiated an excessive amount of such requests, as determined by NTT DATA in accordance with the boundary conditions set out in clause 8.2 below (or other reasonable grounds as NTT DATA may determine under the circumstances) (**‘Fair Use Policy’**). In order to enforce the Fair Use Policy, NTT DATA will monitor Client’s actual usage of the Managed M365 Services against the anticipated or expected usage.

8.2 The following are the boundary target volumes considered a violation of the Fair Use Policy:

Boundary conditions (target volumes)	On a monthly basis, 3% of the Service Units consumed against the combined number of Users and Devices, provided that within this monthly limit, the number of Service Units consumed by Client per day should not exceed a maximum of 0.5% per ratio of number of Users and Devices.
--------------------------------------	--

8.3 At its discretion, NTT DATA reserves the right to invoke the Fair Use Policy, and to review and limit its provisions of Service Requests. In extreme cases, NTT DATA may, with reasonable notice, invoice Client for the services rendered which are deemed to be a violation of the Fair Use Policy or suspend Client’s ability to use the Service Request Fulfilment service feature.

8.4 Service Units are determined or based on the relevant rate card described in the Service Request Catalogue. For the avoidance of doubt, activities that are not listed within the defined scope of the Service Request Catalogue, such as any project-based activities, will be quoted by NTT DATA on a time and materials basis and subject to the parties entering into a separate statement of work.