Co-Management Technology Service Description

Overview

NTT DATA may, where approved and agreed by NTT DATA in the relevant SOW for Managed Campus Network (MCN) Services, grant a limited co-management right to Client, providing Client with additional control and visibility into the Client Network Environment. Where applicable, co-management may be granted to Client on either a role-based access basis or split of responsibilities basis, as specifically detailed in the applicable SOW and described further below.

1 Role Based Access

1.1 Where NTT DATA and Client agree on role-based access, NTT DATA will grant identified Client Users specified role type access to perform changes on the Client Network Environment for such devices that support Role Based Access (RBAC) functionality.

1.2 NTT DATA and Client will define roles and responsibilities for Client identified users and document these in the relevant SOW. Roles may include, but are not limited to, network administrators, network operators or security administrators. NTT DATA will configure read, write, or restricted access permissions for each role type to allow Client to perform activities on specific CIs, CI elements, or CI configurations. Client activities may include:

(a) configuration of CIs; and

(b) changes to routing, switching and security policies.

1.3 NTT DATA will configure its Privilege Access Management (PAM) system to only allow identified roles authorized to perform the agreed activities.

2 Split of Responsibilities

2.1 Where NTT DATA and Client agree on co-management on a split of responsibilities basis, NTT DATA and Client will identify the CIs subject to the co-management and document the type of responsibilities for each CI type/model in the relevant SOW.

3 Co-management conditions

3.1 NTT DATA will deploy and configure the co-management rights, as described in clauses 2 and 3 above and subject to the specific details captured in the relevant SOW, subject (in all cases) to the conditions specified below:

(a) NTT DATA reserves the right to conduct a Network Health Assessment of any devices impacted by the limited co-management rights at any time during the SOW Term to validate the Client Network Environment is still supportable to NTT standards. If NTT DATA determines that the Client Network Environment (or certain devices situated therein) is unsupportable due to changes made by Client, NTT DATA may:

(i) remove or reset the changes implemented by Client that made the Client Network Environment (or certain devices situated therein) unsupportable.

(ii) exclude devices from NTT DATA's Service Level Targets reporting for the duration of when the change was implemented and following the investigation and remediation; and

(iii) deactivate monitoring alerts on the relevant devices to avoid false alarms being generated to remove the changes.

The time incurred (A) for the Network Health Assessment and for corrective actions or changes required to re-align the systems and services, as deemed necessary by NTT DATA, or (B) where Client engages NTT DATA to perform troubleshooting of any issues caused as a direct result of the use of specific access by the Client, will in each case be subject to additional Charges, as determined based on NTT DATA's then-current rates.

(b) Client must raise a Service Request upon making any changes to any of the CIs under split responsibility to allow NTT DATA to have up to date information of the CI state and configuration. The Service Request will contain all necessary information about the changes made.

(c) Client is responsible for creating the named accounts and user groups on the impacted CIs unless NTT DATA is separately contracted to perform such activities.

4 Access records

4.1 NTT DATA will monitor access to Configuration Items and record the Configuration Item access and log audit trail information. At Client's request, NTT DATA will provide Client with access reporting information available in NTT DATA's Privileged Access Management (PAM) system. Client will make such a request through logging of a Service Request.