Service Description: Managed Campus Network Services

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 Managed Campus Network (MCN) Services (the '**Services**').

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. Managed Campus Networks (MCN) Transition-In Period

1 Description

1.1 In relation to the Services, transition refers to the process of moving the Client Network Environment to be under the management and responsibility of NTT DATA, 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 Client must transfer management responsibilities of the Configuration Items to NTT DATA, prior to the migration, deployment, or takeover of a Client Network Environment.

3.2 Client must provide service-specific access to NTT DATA, as described in the Client Connectivity Requirements.

3.3 A Network Health Assessment will be performed on the Client Network Environment either before or during the Transition-In Period, with a resulting report indicating potential security vulnerabilities, outdated software patches or other security risks or concerns that may render certain devices unsupportable. Client is responsible for resolving any risks or concerns raised during the Network Health Assessment in order to prepare the Client Network Environment for takeover by NTT DATA. If needed, Client can request NTT DATA's assistance in the resolution of identified risks or concerns at an additional charge.

3.4 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 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.

3.5 If unable to provide the required information, Client may, at its cost, provide network access for NTT DATA to connect automated discovery tools for the collection of additional Configuration Items and associated attributes required to provide the Services. If requested by Client, NTT DATA will, at an additional charge, conduct a physical on-site discovery exercise in respect of the Client Network Environment for the purpose of collecting Configuration Item information.

4 Assessments conducted by NTT DATA

4.1 On receipt of the information requested to deliver the Services, NTT DATA will review Client's Configuration Items and networking architecture to determine if the Configuration Items can be supported by the Services and will notify Client of any changes required to enable NTT DATA to meet the requirements.

5 Service Portal configuration and access

5.1 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.

Part B. Managed Campus Networks (MCN) Service Features

1 Event management

1.1 NTT DATA will, as further described herein, provide monitoring services for all Configuration Items, using technology-specific monitoring configurations. Monitoring will be performed at a set frequency.

1.2 NTT DATA performs monitoring checks from a data collector hosted near the Client Network Environment. The specific management solution is described in the Client Connectivity Requirements. Once enabled, the monitoring collector automatically recognizes the network devices identified for monitoring and management within the Client Network Environment and starts collecting performance metrics.

1.3 When error conditions are met, alerts are pushed to the event management system for handling by NTT DATA. The platform also continuously captures metrics from the monitored components which are stored and accessed via a graphical user interface (GUI). This information capture is necessary and is used by NTT DATA to perform its Service obligations.

1.4 If an anomaly is detected, the monitoring tools will verify automatically and if the anomaly is persistent, generate an Event. The response to monitoring events will be as follows, depending on the criticality and expected associated action.

Event response	Output
No event, data only	The monitor does not generate an event nor an Incident record. The data is collected only for informational purposes.
All other severities	This will generate an event record that will be managed by the NTT DATA operational processes.

1.5 NTT DATA will, where possible, resolve events automatically; or create an Incident for investigation and resolution.

1.6 NTT DATA will not provide the Service Feature defined in this clause 1 on any part of the Client Network Environment affected by downtime related to:

(a) Scheduled Maintenance or Unscheduled Maintenance (as set out in clause 8 of the Specific Terms); and

(b) any other scheduled downtime, maintenance, changes, or activities initiated by Client (or any of its providers), that impact the delivery of the Services by NTT DATA or lead to excessive alerts being generated.

2 Incident management

2.1 NTT DATA will raise an incident record as a result of Client logging an Incident with NTT DATA through the Service Desk or Service Portal; or after qualification of an event by NTT DATA.

2.2 Following the creation of an Incident record, NTT DATA will respond to Client to confirm the initial Incident classification and prioritization. Incident records will have a priority assigned to them which is determined by the impact and the urgency of the Incident. The table below illustrates how priorities are assigned to Incident records:

Priority assignment		Impact		
		High	Medium	Low
Urgency	High	Priority 1 (P1)	Priority 2 (P2)	Priority 3 (P3)
	Medium	Priority 2 (P2)	Priority 3 (P3)	Priority 3 (P3)
	Low	Priority 3 (P3)	Priority 3 (P3)	Priority 3 (P3)

2.3 Additional description of the priorities is provided in the following table:

Priority Level	Description
Priority 1 (P1)	• Solution availability immediately impacted. • Multiple component failures affecting critical services within the Client Network Environment
Priority 2 (P2)	• Network performance degraded or availability likely to be impacted. • Multiple component failures within the Client Network Environment not affecting network availability.
Priority 3 (P3)	• Incident has the possibility to degrade either performance or availability if not resolved.

2.4 Client may request the escalation of an incident to a higher priority level by contacting an escalation manager through the Service Desk and quoting the reference number.

2.5 NTT DATA may downgrade an Incident if it is being managed to a scheduled timeframe, or resolution has been provided to Client and is in the process of being tested. Where Client initiated the escalation, NTT DATA will obtain Client's approval prior to downgrading.

2.6 Client may request to upgrade a Priority 1 (P1) incident to a Major Incident (MI) by contacting the Service Delivery Manager. The Service Delivery Manager or an NTT DATA Delivery Executive approves this request if it deems it necessary to invoke the Major Incident management process. During this process, multiple engineering teams may be involved in the Incident resolution and Client is continually notified of the resolution progress. An NTT DATA Delivery Executive may also decide to invoke the MI process, without Client requesting it, to expedite the resolution of an Incident.

2.7 On conclusion of the Major Incident management process, a problem record is logged to determine the cause of the Major Incident through the problem management process (see Part B, clause 7 below).

2.8 NTT DATA will remotely diagnose the cause of the Incident and resolve the Incident or put a workaround in place and update Client on progress and closure of the Incident.

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

2.10 Incidents without a response from Client are eventually closed. NTT DATA will update the Incident record requesting Client's answer every 3 days. After the third failed attempt the Incident record will be set to a restored state. If Client does not reactivate the Incident within 7 days, the Incident will be automatically closed.

2.11 Incidents with impact where 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.

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

2.13 Incidents logged by Client will be closed automatically if the incident relates to any part of the Client Network Environment affected by any of the downtime scenarios described in clause 1.6 of this Service Description above.

3 Service Request fulfillment

3.1 NTT DATA will raise a Service Request record as a result of Client logging a Service Request through the Service Desk or Service Portal, or as part of the performance of NTT DATA's obligations in relation to performance of a Service Feature.

3.2 Following the creation of a Service Request record, NTT DATA will respond to Client to confirm the initial Service Request classification.

3.3 In-scope Service Requests, as described in the Fair Use Policy set out in clause 9 of the Specific Terms are considered part of the Services offered and therefore, do not incur an additional charge. These requests will be processed after NTT DATA has received all pertinent information.

3.4 The specific Service Requests that are included or excluded as part of the Services will be detailed in the Request Catalogue applicable to the contracted Services, as set out and incorporated in the SOW.

3.5 If NTT DATA determines that Client has requested activities that are not in-scope of the contracted Services, the following process will apply:

(a) NTT DATA will notify Client that the Service Request is not in-scope and may therefore be subject to additional charges;

(b) if the requested activities are subject to additional charges, NTT DATA will notify Client. NTT DATA and Client will agree upon the associated cost for the requested out-of-scope activities; and

(c) once written approval is received, NTT engineers will proceed with the Service Request.

3.6 NTT DATA reserves the right to suspend or re-schedule any Service Request that requires (or is likely to result in) an interruption of the Services, and therefore needs to be fulfilled within a maintenance window.

3.7 NTT DATA reserves the right to suspend any Service Request that implies a change to the scope of the contracted Services. Such change will be treated as a new project and may be subject to additional charges.

4 Availability management

4.1 NTT DATA will monitor for the Availability of Configuration Items using NTT DATA-specific monitoring tools.

4.2 NTT DATA will, where possible, resolve Availability events automatically; or create an Incident for investigation and resolution through the Incident management process, described in Part B, clause 2 of this Service Description.

4.3 NTT DATA will make Availability statistics available on the Service Portal. The statistics and reports provided, as part of the Services, are listed in Part D of this Service Description.

4.4 NTT DATA will, periodically, analyze the available data to assess where a Configuration Item's Availability could be improved.

4.5 Any Availability improvement recommendations will be provided to Client as part of the monthly reporting, and will include:

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

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

5 Capacity and performance management

5.1 NTT DATA will monitor for the capacity and performance of Configuration Items using NTT DATA-specific monitoring tools.

5.2 NTT DATA will, where possible, resolve capacity and performance events automatically; or create an Incident for investigation and resolution, through the Incident management process, described in Part B, clause 2 of this Service Description.

5.3 NTT DATA will make capacity statistics available on the Service Portal. The statistics and reports provided, as part of the Services, are listed in Part D of this Service Description.

5.4 NTT DATA will, periodically, analyze the available data to assess where a Configuration Item's capacity and performance could be improved.

5.5 Any capacity and performance improvement recommendations will be provided to Client as part of the monthly reporting, and will include:

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

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

6 Service asset and configuration management

6.1 NTT DATA will record the Configuration Items in the Service Management System during the Transition-In Period and update the information through the change management process set out in Part B, clause 8 below.

6.2 NTT DATA will, through its or Manufacturer data sets, enrich the Client-provided Configuration Item data with additional, applicable information.

6.3 NTT DATA will provide Client with access to the enriched Configuration Item information through the Service Portal.

7 Problem management

7.1 NTT DATA continuously detects and aggregates the most repetitive alerts and events through its monitoring tools.

7.2 NTT DATA will raise a Priority 1 (P1) problem record, where applicable:

(a) to find the root cause of one or more Priority 1 (P1) incidents that do not have a permanent resolution in place; or

(b) to determine the cause of a Major Incident.

7.3 NTT DATA will raise a Priority 2 (P2) problem record, where applicable, for analysis of available data to identify the cause of the top 5 Events repeated in a 30-day period.

7.4 NTT DATA will provide a Root Cause Analysis (RCA) report to make recommendations and, at Client's request, implement the recommendations (depending on the scope):

(a) in accordance with the request fulfilment process as set out in Part B, clause 3 above for all in-scope Service Requests;

(b) at an additional charge (on a time and materials basis) for out-of-scope Service Requests; or

(c) pursuant to 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.

8 Change management

8.1 NTT DATA will raise a change request record as a result of Client logging a Service Request through the Service Desk or Service Portal, or as part of the performance of NTT's obligations under a Service Feature.

8.2 Following the creation of a change request, NTT DATA will assess the change to determine the type and classification based on the impact and risk of the change. NTT DATA will manage the lifecycle of a change request in accordance with the change type and classification.

8.3 NTT DATA will make the results of the change impact and risk analysis available to Client. Client may request the escalation of a change request to a higher impact level by contacting the Service Desk and quoting the reference number.

8.4 Changes are approved by a change manager or a Change Advisory Board (CAB), depending on the classification of the change. Client will retain accountability for the CAB. Where the Client does not have a CAB, Client will appoint a representative to approve changes on behalf of Client.

8.5 The table below illustrates how types of changes are assigned:

Change Type	Description
Standard	A low risk, templated change that has been included in the request catalogue and is repeatable because there is an associated procedure for implementing and rolling back the change. The change is logged as a Service Request and follow the request fulfilment process. NTT DATA can evaluate any change request in terms of the change duration, the change impact, and the level of technical detail and skill required to implement the change to determine if it can be implemented at the level requested. If found to be more complex than originally requested, or the effort required to implement the change is more than 16 hours, it can be submitted through the normal change process.
Normal	All changes that are not defined as type 'Standard' are normal changes and classified as per the table set out in Part B, clause 8.6 below. These changes have no predefined procedure and requires approval, as the table set out in Part B, clause 8.7 below.

8.6 The table below describes how the classification of changes is assigned:

Change classification		Risk				
		Very High	**High**	**Moderate**	**Low**	**None**
Impact	**Total loss**	Major	Major	Significant	Minor	Minor
	Degradation	Major	Significant	Significant	Minor	Minor
	No Impact	Minor	Minor	Minor	Minor	Minor

8.7 Additional description of the change classification for normal changes is provided in the following table:

Change classification	Description
Major	Changes where a critical part of the Client Network Environment are impacted or at risk. The change requests need a lead time of at least 10 days prior to implementation for assessment and approval through the CAB.
Significant	Changes where a significant part of the Client Network Environment are impacted or at risk. The change requests need a lead time of at least 7 days prior to implementation for assessment and approval through the CAB.
Minor	Changes where the impact and risk factor are not identified as major or significant and where the change manager can approve these changes without submitting them to the CAB.

8.8 Where business impact criteria are justified, the assessment and approval of normal changes can be expedited, having different lead times than what is described in the table set out in Part B, clause 8.7 above.

8.9 The table below describes the criteria for urgent and emergency change approval types:

Change approval type	Description
Urgent	An urgent change is a normal change with an expedited approval process for business reasons: • to fix high priority incidents, where redundancy is in place; • to prevent a possible outage; • where there is a business impact if the change is not implemented; and • for project changes, where the change required was omitted during planning and the change is needed to prevent delays in the project (only valid where other activities of the project are already scheduled for change implementation).
Emergency	An emergency change is a normal change that needs to be implemented immediately to fix an Incident or restore a Service.

8.10 The lead time for urgent change approval for each change classification is:

(a) 2 business days for a major change;

(b) 1 business day for a significant change; and

(c) 8 business hours for a minor change.

8.11 The maximum number of urgent changes that can be implemented is 3 per calendar month or 1 for every 1000 Configuration Items under management, whichever is greater, and up to a maximum of 50 CIs per change.

8.12 Emergency changes (as described in the table set out in Part B, clause 8.9 above) are approved by a Client representative who can be contacted 24x7 along with the Service Delivery Manager. Emergency changes are logged in the Service Management System retrospectively.

8.13 NTT DATA will produce a change plan (with input from Client) for change requests, that includes:

(a) a test plan for testing the change prior to roll-out;

(b) a test plan for testing the change after the roll-out;

(c) tasks for the implementation of the change;

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

(e) calculation of the time required to implement the change.

8.14 NTT DATA will submit the change plan to Client for approval and for submission to the CAB, if applicable.

8.15 NTT DATA will, upon receipt of approval from Client, proceed with testing of the change in a non-production environment of Client or on a live Configuration Item agreed by Client, at Client's risk. If testing of the change is not possible, Client will assume the risk of implementing the change.

8.16 NTT DATA will, after testing of the change, where applicable, implement the change according to the approved change plan. Standard changes are included and considered the same as in-scope Service Requests. Significant and major changes may, depending on the scope of the changes:

(a) incur additional charges on a time and materials basis; or

(b) require 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.

9 Release and deployment management

Emergency Patches and Operational Releases

9.1 From the Service Commencement Date, NTT DATA will regularly check for critical security advisories that affect the supported technologies within the relevant Client Network Environment.

9.2 NTT DATA will analyze and determine the criticality of an identified vulnerability against the Client Network Environment and if a vulnerability is declared a threat or to have a high risk of outage, the associated patch will be deemed an emergency ('**Emergency Patch**'), and NTT DATA will inform the Client within 2 business days of identifying the vulnerability. Subject to timely receipt of Client's approval, NTT DATA will implement the Manufacturer-provided Emergency Patch (or workaround) within 48 hours of initially notifying Client of the vulnerability (unless Client requests installation in a specific, scheduled change window).

9.3 Should NTT DATA identify a resolution to an Incident or problem as a patch or release upgrade ('**Operational Release**'), NTT DATA will implement the Operational Release in accordance with the incident management or problem management processes set out above (as applicable).

9.4 While Emergency Patches and Operational Releases will be counted towards the release and deployment management limits set out in clause 9.10 below, there is no cap on the number of Emergency Patches or Operational Releases that NTT DATA will perform as part of the Services, and NTT DATA will implement all Emergency Patches or Operational Releases where deemed necessary pursuant to the terms of clause 9.2 and 9.3 above (respectively).

Vulnerability assessments and Standard Patches

9.5 In addition to the checks described in clause 9.1 above, NTT DATA will perform a patch and vulnerability assessment once every 3-month period, commencing 90 days after Service Commencement Date.

9.6 Following each patch and vulnerability assessment, NTT DATA will:

(a) provide Client with the assessment results and relevant Manufacturer notification information for in-scope Configuration Items through the Service Portal, including recommended software versions and associated security advisories (if applicable); and

(b) recommend actions to be taken based on the assessment results (which could include the recommendation to do a more detailed investigation).

9.7 Subject always to the limitations set out in clause 9.10 below, NTT DATA will install any agreed patches ('**Standard Patches**') identified through the standard patch and vulnerability assessment once every 3-month period (except, as may be notified by NTT DATA, where a longer timeframe is required due to the number of patches or size of the environment).

9.8 NTT DATA will follow the standard change management processes to implement Standard Patches.

Reporting

9.9 NTT DATA will report on all patches and releases implemented once every 3-month period.

Release and deployment management limits

9.10 NTT DATA will, as an included feature of the Services, implement:

(a) 1 Major Release; and

(b) 2 Minor Releases or Patches (of any type);

per Configuration Item in any 12-month period, with all Emergency Patches and Operational Releases being counted towards the foregoing limits (but not otherwise being subject to volume restrictions set out in this clause 9.10).

9.11 Any additional support (including the implementation of patches or releases above the limited set out in clause 9.10) will be subject to additional charges on a time and materials basis. Estimated cost of implementation can be provided by NTT DATA upon Client's request.

Exclusions

9.12 NTT DATA can only provide the Service Feature defined in this clause 9 where notification from the relevant Manufacturer is received. Where the Manufacturer does not provide notifications in respect of a Configuration Item, NTT DATA will not be liable for performance of this Service Feature.

9.13 Information displayed on the Service Portal will be limited to that received through Manufacturer provided notification services (as subscribed to and automated by NTT DATA as part of the Services).

9.14 NTT DATA is not responsible for the functionality and applicability of any Manufacturer-provided release packages and patches.

9.15 Where a release includes modification of configuration, ways of working, or functionality of the device, NTT DATA is not responsible for such adaptations (which will remain the responsibility of Client). Where requested by Client, NTT DATA can provide additional services to uplift the capability to support the new release subject to additional charges on a time and materials basis.

10 Service level management

10.1 NTT DATA will provide an interface, the Service Delivery Manager, who will manage the service delivery relationship between NTT DATA and Client, provide a key point of escalation for Client, and conduct service management review meetings to review operational and business performance of the Services provided.

10.2 The service management review meetings occur on a schedule mutually agreed to by Client and NTT DATA, and are designed to allow for a regular review of:

(a) monthly Service Level Target achievements and other key performance indicators;

(b) Major Incidents from the previous month and any associated service improvement activities required to prevent re-occurrence or improve the Services;

(c) identified problems, root cause analyses, known errors and permanent fixes planned;

(d) changes implemented within the previous month and highlighting any issues or concerns with the planning or implementation of changes;

(e) potential areas of escalation or concern and action plans to remediate; and

(f) identification of any tactical improvements to service delivery.

11 Access management

11.1 NTT DATA will deploy and configure devices with the users and associated level of administrative rights required to provide the Services. Subject only to the specific exceptions set out in Part B, clause 11.2 below, NTT DATA will be the only party having administrative rights on all items under management.

11.2 Notwithstanding the general restrictions on administrative rights described in Part B, clause 11.1 above, NTT DATA:

(a) will provide Client with an administrative account which may be used in the event NTT DATA is unable to deliver or provision the Services due to Force Majeure;

(b) may, if special business requirements justify a shared management model whereby the Client or a Third-Party Supplier requires administrative rights, grant such rights for an interim period

(c) provided in the case of both (a) and (b) above, the following caveats shall apply:

(i) NTT DATA's Service Level Targets will not apply during the relevant period;

(ii) monitoring alerts may be deactivated to avoid false alarms being generated by the Client or Third-Party Supplier activity on the devices or service components;

(iii) in cases where Client or Third-Party Supplier engages NTT DATA to perform troubleshooting of any issues caused as a direct result of the use of administrative rights by the Client or Third-Party Supplier, such activity may be subject to additional charges; and

(iv) once the relevant period is over and NTT DATA has been requested to resume the Services, NTT DATA reserves the right to conduct a Network Health Assessment of the affected devices to validate the Client Network Environment is still supportable. The time incurred 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, may be subject to additional charges. The changes implemented by Client or Third-Party Supplier may also be removed, if deemed necessary to ensure supportability of the devices.

11.3 Client will follow the service request fulfilment process, as set out in Part B, clause 3 above, to log a request for access to a Configuration Item.

11.4 Where a Service Request for access has been raised by Client to modify end user access rights (grant access, restrict access or revoke access) to a Configuration Item, NTT DATA will verify the identity of the end user (or requestor if not the end user) through:

(a) username/password authentication;

(b) informal identification such as the email address used in the access request; or

(c) such other form of identification as agreed with Client.

11.5 On successful verification of a Service Request for access authorization, NTT DATA will:

(a) modify the end user's access in accordance with the request; and

(b) notify both the end user and authorizing authority once access has been modified.

11.6 NTT DATA will monitor access to Configuration Items; and record the Configuration Item access and log audit trail information.

11.7 NTT DATA will, at Client's request, provide Client with access reporting information. Client will make such a request through logging of a Service Request as per Part B, clause 3 above.

12 IT service continuity management

12.1 Where Configurations Items are monitored and accessible remotely, NTT DATA will, where applicable:

(a) for backup of CI configuration files:

(i) backup a Configuration Item's configuration file; and

(ii) store one current and five historic versions of Configuration Item configuration files;

subject, in each case, to the more specific backup policies (including any size thresholds) and limitations set out in the relevant Technical Service Description; and

(b) for Release and Deployment Management (as described in Part B, clause 9):

(i) transfer software packages received from vendors to a storage location; and

(ii) deploy the software package to the applicable Configuration Item;

subject, in each case, to the more specific policies and limitations described in Part B, clause 9.

12.2 Where NTT DATA provides the backup infrastructure (in support of the functions described in clause 12.1(a)) or release and deployment infrastructure (in support of the functions described in clause 12.1(b)), additional cost for bandwidth and storage will apply.

13 Supplier management

13.1 Where an incident occurs within the Client Network Environment to a Configuration Item that is managed by NTT DATA, but the responsibility for repair falls under a Third-Party Supplier (including, without limitation, an OEM or carrier circuit provider) NTT DATA will assist these Third-Party Suppliers with resolution via a letter of authorization (LOA) with these Third-Party Suppliers, subject to the restrictions in Part B, clause 13.2 below and any specific carrier coordination policies set out in the relevant Technical Service Description, when Carrier Coordination is purchased.

13.2 Where the restoration of an incident on a Configuration Item falls within the scope of services provided by a Third-Party Supplier, the following will apply:

(a) NTT DATA will log the incident to the Third-Party Supplier for resolution on behalf of Client, where the Third-Party Supplier has signed an LOA and provided access for NTT DATA to log the incident NTT DATA will provide assistance to the Third-Party Supplier, on behalf of Client, until the incident is resolved and closed;

(b) NTT DATA is not responsible for dispatching, safe storage, disposal or return of any Configuration Item or spare parts from the replacement of a Configuration Item;

(c) NTT DATA is not accountable or responsible for any resolution activities or access, safety and logistical requirements of the field engineers performing the on-site incident resolution activities;

(d) NTT DATA is not accountable or responsible to meet restoration Service Level Targets with the Third-Party Supplier. The standard Incident Management Service Level Targets will apply for the in-scope Service Features, excluding the incident restoration Service Level Targets. Restoration Service Level Targets will be paused for the related Configuration Items once the Third-Party Supplier has been notified;

(e) NTT DATA will provide progress update notifications to Client only as and when received by the Third-Party Supplier;

(f) NTT DATA will not be responsible to identify, provide or report on the root cause of the incident;

(g) NTT DATA will not be responsible for any invoice or billing related queries or requests related to the Third-Party Supplier provided services;

(h) Client must provide any access to a support portal, escalation matrices, contact details, Configuration Item attributes and relationships or other details that may be necessary for NTT DATA to coordinate the incidents to resolution with the Third-Party Supplier;

(i) NTT DATA is not responsible or accountable for any deliverables or obligations from any agreement between the Client and Third-Party Supplier, except where NTT DATA is responsible for this as part of its contractual obligations to Client under a Service Feature; and

(j) Client must present the LOA to the Third-Party Supplier and obtain the necessary signatures.

13.3 If, under the applicable circumstances, an NTT DATA Affiliate is the relevant Third-Party Supplier pursuant to this Part B, clause 13, an LOA is not required, but the other terms of Part B, clause 13.2 still apply.

14 Service Experience Insights

14.1 Where the scope of Services set forth in the applicable SOW expressly includes Service Experience Insights, NTT DATA will provide Client with vendor agnostic monitoring of agreed business-critical services from different points on a network managed by NTT DATA, subject to the more specific policies and limitations set out in the relevant Technical Service Description.

14.2 In order to provide Service Experience Insights, NTT will, as agreed by the parties, either install a software agent on a Client network CI or utilize NTT DATA's MCN Edge Appliance to provide the Service Feature.

14.3 If, through the Service Experience Insights configuration, an anomaly is detected, the alert will be managed in accordance with the Event management process described in Part B, clause 1 of this Service Description.

15 Guest Wi-Fi Enablement

15.1 Where the scope of Services set forth in the applicable SOW expressly includes Guest Wi-Fi Enablement, NTT DATA will provide Client with a cloud-native guest Wi-Fi solution to manage their guest Wi-Fi and provide corresponding analytics. Guest Wi-Fi Enablement leverages Client's campus Wi-Fi technology stack and includes the features, and is subject to the more specific policies and limitations, set out in the relevant Technical Service Description.

16 Managed Log Management

16.1 Where the scope of Services set forth in the applicable SOW expressly includes Managed Log Management, NTT DATA will provide Client with a central server to send system logs or event messages to be displayed on the Service Portal. The provision and use of Managed Log Management is subject to the more specific policies and limitations set out in the relevant Technical Service Description.

17 Managed Advanced Security

17.1 Where the scope of Services set forth in the applicable SOW expressly includes Managed Advanced Security, NTT DATA will provide security features on Client's security appliance, as well as subject-matter-expertise to manage the advanced security features of their security appliances and Secure Access Service Edge (SASE) solution. The provision and use of Managed Advanced Security is subject to the more specific policies and limitations set out in the relevant Technical Service Description. Client will follow the service request fulfilment process to log a request for access to a subject matter expert in connection with the Managed Advanced Security service.

Part C. Managed Campus Networks (MCN) Service Portal

1 Service Portal description

1.1 NTT DATA will deliver a single view of the Client Network Environment under management, regardless of the locations in which physical and logical assets are based, using its Service Portal. The Service 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 Service Portal attributes

2.1 The primary attributes of the Service 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 support team via ticketing system;

(d) visibility of the CMDB; and

(e) tracking of Incidents and Incident resolution

Part D. Managed Campus Networks (MCN) Reporting

1 Service Management Reports

1.1 The following table specifies all Service Management Reports to be provided as part of the Services, and their respective methods of delivery and frequency:

Service	Content of Report	Delivery	Frequency
Managed Campus Network Services	Operations summary including information on: ● Service levels achievement ● Change management ● Configuration and Inventory incl. End-of-X milestones ● Request fulfilment ● Problem management	**Monthly service review meeting** (and subsequently made available at the Service Portal)	**Monthly**

Availability Management Statistics	Statistics and Reports on: ● Interfaces with errors ● Interfaces with discards ● Availability problems per configuration item type ● Infrastructure Availability summary ● Reachability problems ● Automated Service Management Report ● Service Availability Report (if configured)	**Service Portal**	**Near Real-time**
	● Patch Assessment Report* ● Vulnerability Assessment Report* **based on supported vendor list*	**Service Portal**	**3 Monthly**
Availability Management Analysis and Recommendations	Recommended actions on how to improve Availability of Client Network Environment ● Top Availability problems ● Interface Analysis	**Report**	**Monthly**
Capacity Management Statistics	Statistics and Reports on: ● Interface bandwidth utilisation ● Processor utilisation ● Memory utilisation ● Storage utilisation ● DVR Playback Report	**Service Portal**	**Near Real-time**
Capacity and Performance Management Analysis and Recommendations	Recommended actions on how to improve Availability of Client Network Environment	**Report**	**Monthly**

2 Self-service reporting

2.1 A standardized set of self-service dashboards and access to data for the Services are available on the Service Portal. This allows the Client to generate its own charts and to access graphs and change scales where needed. Reporting data will be available via the Service Portal within 30 minutes of the live event.

2.2 NTT DATA will provide Client with availability, capacity and performance data, including statistical information in respect of availability events on the Service Portal.