SERVICE DESCRIPTION

Device Management Enhanced

Name	NTT Service Description – Device Management Enhanced
Owner	NTT
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.2
Date	29 March 2019

Contents

1 Service Matrix

The Device Management Enhanced service consists of a core set of Service Modules and associated Service Elements.

Section	Service Modules and Elements	Device Management Enhanced
3	Core Service Elements	
3.1	24/7 Hours of Operation	✓
3.2	Security Operation Centers	✓
3.3	NTT Portal	✓
3.4	Language Support	✓
3.5	Management of Devices	✓
3.6	Communications	✓
3.7	Escalation Management	✓
4	Service Transition	
4.1	Engagement	✓
4.2	Planning	✓
4.3	Staging	✓
4.4	Integration	✓
4.5	Go-Live	✓
5	Device Management Features	
5.1	Health and Availability Monitoring	✓
5.1.1	Health and Availability Monitoring	✓
5.1.2	Health and Availability Improvement and Recommendation	✓
5.1.3	Health and Availability Change Implementation	✓
5.2	Incident Management	
5.2.1	Incident Generation	✓
5.2.2	Incident Diagnosis	✓
5.2.3	Incident Resolution	✓
5.2.4	Incident Reporting	✓
0	Capacity Management	
5.3.1	Capacity monitoring and reporting	✓
5.3.2	Capacity improvement recommendation	✓
5.3.3	Capacity Planning	✓
5.3.4	Capacity Change Implementation	✓
0	Asset Tracking and Reporting	
5.4.1	Configuration Item Recording	✓
5.4.2	Configuration Item Control and Updates	✓
5.4.3	Configuration Item Backup	✓
5.4.4	Configuration Item Restore + OOB	✓
5.4.5	Configuration Item Status Reporting	✓
5.4.6	Co-Management	Optional
5.5	Optional 5.5 Service Request Fulfilment	
5.5.1	Service Request Management	✓
5.5.2	Move, Add, Change, Delete (MACD) Fulfillment	✓
5.5.3	Change Management	✓
5.6	Problem Management	
5.6.1	Problem Identification and Recording	✓
5.6.2	Problem Reporting	✓
5.6.3	Solution Identification and Recording	✓
5.6.4	Solution Implementation	✓

2 Service Prerequisites

2.1 General Requirements

2.1.1 In all cases

The standard delivery model shall be 24 hours a day, 7 days a week leveraging NTT Ltd. SOCs. Deviation from this standard shall only be considered on a case by case basis and must be supported by a completed application for non-standard services. NTT Ltd. shall consider the request, any cost implications and wherever possible shall strive to meet the requested requirements. However, NTT Ltd. reserves the right to refuse any request for deviation from the standard delivery model.

2.1.2 Configuration Item

An NTT Ltd. supported configuration item to be managed by the service.

2.1.3 Software/appliance license

Client is responsible for a valid manufacturer product license(s) which is required for all components (including security application and operating system) of the configuration item under management for the duration of the NTT Ltd. Service contract period. The Client must ensure that licenses are valid at the start of the NTT Ltd. service contract through to the end of the NTT Ltd. service contract.

2.1.4 Manufacturer Hardware/Software Support

Managed configuration items must have full manufacturer support at all times during the NTT Ltd. service contract period. The manufacturer support contract must have Partner Enablement where applicable. NTT Ltd. must be added as an authorized vendor support contact and/or Partner in order to raise support tickets with the manufacturer on the Client's behalf. NTT Ltd. will not provide any services for any configuration item not covered by a valid maintenance contract.

Neither shall NTT Ltd. manage any configuration item where the software or hardware has been declared 'end of life' or 'end of support' by the manufacturer, prior to the start of any NTT Ltd. contract or subsequent 12-month renewal period. Replacement of obsolete hardware/software is not included in the service.

2.1.5 Software Updates (Subscriptions)

The Client is responsible for all Manufacturer’s Software Subscriptions (i.e. software updates) for any configuration items to be managed. Such subscriptions are required for the duration of the NTT Ltd. service contract period. The Client must ensure that any software subscriptions are valid at the start of the NTT Ltd. service contract through to the end of the service contract. NTT Ltd. will not provide any services for expired subscriptions.

2.1.6 Limitations of use

Only the manufacturers’ security application/operating system software, relevant and/or necessary software/applications and software provided by NTT Ltd. (where applicable) to support the NTT Ltd. service are to be run on the configuration item.

2.1.7 Secure System Management

The in-scope configuration item(s) must have a secure configuration/policy that is agreed between NTT Ltd. and the Client which is implemented prior to the start of any NTT Ltd. service contract (including renewals). This must be maintained for the full-service period.

2.1.8 Secure facility

It is the Client’s responsibility to provide and maintain a physically secured and environmentally suitable facility for any manufacturer hardware/software and associated NTT Ltd. supplied hardware/software including appropriate rack space and power.

2.1.9 Virtual environment

All virtual environments provided by the Client for the NTT Appliance must adhere to specifications outlined within the latest ‘NTT Appliance Installation and Configuration Guide’ which can be found on the NTT Portal. In addition, proactive monitoring of any shared resources (CPU, memory, network and storage) is the responsibility of the Client to ensure a stable virtual environment. Any hardware or software issues relating directly to the virtual environment are the Client’s responsibility, however NTT Ltd. will work with the Client to resume normal operations in the event of appliance related failures.

2.1.10 Designated Security Contacts

The Client must provide at minimum two staff members to be the security contacts and if applicable a Service Desk contact that NTT Ltd. will liaise with to deliver the Device Management Service. Full contact and authentication details for each of the security contacts must be provided by the Client and included within the Client Security Service Detail (CSSD).

2.1.11 Administrative Privileges

NTT Ltd. requires full and exclusive administrative, root or read-write privileges for all in-scope configuration items for the service contract period. Where a co-managed service has been purchased and mutually agreed, should the Client disable such privileges either intentionally or in error, at any time, NTT Ltd. reserves the right to suspend services for applicable configuration items until the situation is remedied. In such cases no claim for service credit shall be applicable. NTT Ltd. is not responsible for any Incident involving an in-scope configuration item while such privileges are disabled or otherwise non-functional.

2.2 Communication Requirements

2.2.1 NTT Appliance

Managed Security Services require an NTT Appliance.

The NTT Appliance is available in multiple form factors which includes both virtual and physical hardware, all of which must be installed, initially configured and enrolled by the Client. NTT Ltd. will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors) and the physical appliance form factor if supplied by NTT Ltd.

NTT Appliances gather Logs, events, reports, and evidence data from in-scope Client devices and systems, then prepare the data for secure transmission and processing. The NTT Appliance also provides a secure communication path for Device Management service delivery. Ongoing configuration and maintenance of the NTT Appliance is conducted by NTT Ltd. and therefore the appliance must be installed by the Client in a suitable location on the Client network infrastructure to facilitate both NTT Ltd. access and log collection.

The NTT Appliance requires:

- At least one static (non-dynamic) IP address
- Permanent LAN Connectivity
- Permanent internet connectivity on TCP port 443

For the virtual form factor the appliance also requires:

- Configuration to power on automatically if the hypervisor is restarted
- Minimum resources from the hypervisor in the virtual environment as specified by NTT Ltd.

2.2.2 Configuration Item Requirements

All in-scope configuration items require:

- For internet facing configuration items a static (non-dynamic) public IP address
- For non-internet facing configuration items – a static (non-dynamic) RFC 1918 IP address
- Necessary network connectivity to NTT Appliance as specified by NTT Ltd.

2.2.3 Connection to Client Network

The Client must supply all the necessary network hardware and cabling to connect the configuration item to the Client's own, third party and ISP networks. All network interfaces connecting to the configuration items must be a minimum of 1 Gigabit Ethernet interfaces. The standard for Gigabit stipulates auto mode as mandatory. However, some manufacturers have deviated from this and do facilitate the hard coding of interface speed and duplex. Where this is enabled, it is imperative that both ends of the network cable are set to fixed speeds and duplex modes (in other words both Switch and Configuration Item). In this instance it is important that the Client discusses any potential infrastructure changes that may affect this setting during the Service Transition process or directly with the SOC during service operation.

2.2.4 Out of Band Management

Remote Management Kit (RMK) provides Out of Band (OOB) console access and power management of in-scope configuration items. The RMK is deployed to premises where Client infrastructure is located and integrated with in-scope configuration items. It is not applicable or supported for virtual or cloud-based configuration items. Provision of an RMK allows NTT Ltd. to provide a device uptime OLA if there is secondary connectivity and the Client has not opted for co-management. RMK is mandatory for the Device Management Enhanced offering (where applicable).

RMK requirements and options:

- Primary In-Band IP connectivity to Client infrastructure is via the NTT Appliance through an auto established VPN maintained by NTT Ltd.
- Secondary Out-Of-Band connectivity is via one option from the table below, supplied and maintained by the Client:

Connectivity Option
Secondary internet circuit (Per site)
3GPP/3GPP2 cellular via 2FF Mini SIM (ISO/IEC 7810:2003, ID-000) with data plan (Per RMK)
Dedicated ADSL to the internet (Per RMK)
Wi-Fi to the internet (Per site)

The RMK provides power management of configuration items through inline serial-controlled Power Modules.

A connection to a power supply is required per RMK and must be separate to the power management options above.

3 Core Service Elements

3.1 Hours of Operation

Managed Security Services are delivered through the Security Operations Centers (SOCs) of NTT Ltd. Unless otherwise stated MSS hours of operation are 24 hours a day, 7 days a week.

3.2 Security Operation Centers (SOCs)

NTT Ltd. will deliver services through its SOCs. NTT Ltd. may at its sole discretion deliver services through any of its SOCs, and Client data may be held in any SOC and/or NTT Ltd. Infrastructures unless there is prior agreement and approval between NTT Ltd. and the Client for data to be held in any reduced subset of the above. The Client will be provided with the contact details of relevant SOCs through the Service Transition process.

3.3 NTT Portal

The NTT Portal is a globally available web-based application, which allows Clients to interact with, manage, and monitor our Managed Security Services.

3.4 Language support

Services are provided in English language only, unless there is prior agreement and approval between NTT Ltd. and the Client.

3.5 Management of Devices

Management of devices is included within the Device Management Enhanced service offering with responsibilities dependent on the type of management selected by the Client, as outlined below.

3.5.1 Management

Management is included as a core component of the Device Management Enhanced service offering where the Client provides NTT Ltd. with privileged access to configuration item(s) within scope. The Client does not have any access to configuration item(s) within scope unless the Co-Management Add-On (see 3.5.2) is purchased or Read-only access is requested (see 3.5.3).

NTT Ltd. will create one administrator account (Break Glass account) for Client and will securely store the credentials and password. In the event of an emergency where NTT Ltd. is unable to make a Change or access the configuration item/management infrastructure, the primary Client security contact will be provided with the credentials and password.

Each time the Client uses the Break Glass account, NTT Ltd. resets the account with a new password.

Except with Co-Managed configuration items, the Client agrees not to create any administrator or other change-capable accounts (i.e. 'super user') on 'in-scope' configuration items. If required, The Client must request creation of such administrator accounts via the NTT Portal. NTT Ltd. performs periodic and ongoing auditing of all administrator accounts.

3.5.2 Co-Management

Co-Management is a chargeable add-on to the Device Management Enhanced service offering. NTT Ltd. and the Client and/or its nominated third party and/or an NTT Ltd. Group Operating Company have access to in-scope configuration item(s) with the ability to make updates and configuration changes. In a Co-Managed scenario specific conditions apply, see 5.4.6.

3.5.3 Read-only Access

The Client can be provided with read-only access to configuration item(s) within scope if requested during Service Transition or via the NTT Portal.

3.6 Communications

3.6.1 MSS Infrastructure

NTT Ltd. utilize a regional-based infrastructure with security by design principles built in, it is highly resilient and secured using best practice methodologies tools and techniques. It is fully managed by our Global Services staff and monitored using our DM, ESM and TD security services.

3.6.2 Notifications

3.6.2.1 Email

For security and data privacy reasons, email notifications will only contain minimal information to notify Clients about creation of, updates to and closure of Cases. Such emails shall not contain any sensitive information apart from the appropriate ticket reference number (and where possible not to disclose any private information a short description of the ticket).

Clients may send emails relating to new or existing Cases to NTT Ltd. In the case where no reference number is provided as formatted by NTT Ltd., we shall create a Case with a short description based on the subject line provided.

When a Client is replying to an email with an existing reference number (as provided by NTT Ltd. and unchanged by the Client), the message body text shall be copied (upon receipt) to the journal of the relevant Case and shall be marked as updated by the customer and waiting on NTT Ltd.'s further input. For security reasons, if Clients wish to send sensitive information to NTT Ltd. or provide approval workflow pertaining to an existing or new incident or request, they are urged to do so using the NTT Portal.

3.6.2.2 File attachments

Diagrams, images, PDFs, executables and any other attachments must not be attached to any Case via email. Where file attachments are necessary, the Client must log in to the NTT Portal and attach the file securely through their web browser connected to the NTT Portal.

3.6.2.3 Telephone

SOC staff may contact Clients and Clients may contact SOCs by telephone. In both cases an authentication shall be completed to verify Client identity.

3.6.2.4 NTT Portal

Unless otherwise stated and agreed, all other communications originating from our SOCs shall be secure and follow security best practices via the NTT Portal.

3.6.3 ITSM (Service Management) Tool

Our ITSM module manages Cases aligned with ITIL wherever appropriate. Access is provided to appropriate NTT Ltd. staff only.

3.6.4 Monitoring

3.6.4.1 Protocols

Client configuration items are monitored utilizing multiple protocols including SNMP v2, v3, SSH v2, HTTP, HTTPS and ICMP.

3.6.4.2 Health and Availability Monitoring Events

The event feeds from in-scope configuration items are sent to the NTT Appliance and securely sent via a VPN to the monitoring server in the MSS infrastructure.

3.6.5 Engineering

3.6.5.1 Configuration Item Access

Command line access is secured via SSH v2. SSH Access is provided from a trusted NTT Ltd. 'jump host' within the MSS infrastructure that leverages the VPN established from the NTT Appliance.

3.6.5.2 Application Access

Application specific protocols to access management consoles within Client premises are secured using SSH v2 and HTTPS from NTT Ltd. 'jump hosts' leveraging the VPN established from the NTT Appliance.

3.6.5.3 Backup

A backup server is located within the MSS Infrastructure and communications secured over VPN to the in-scope configuration item(s). The backup server is utilized to take backups of configuration item(s) in scope and is encrypted and stored within MSS infrastructure.

3.6.5.4 OOB

Out of Band access is provided for configuration item management in the event of an availability affecting event to facilitate bare metal restore or critical management capabilities during an outage. It is only applicable and supported when access to a physical supported configuration item or chassis is available.

3.7 Escalation Management

NTT Ltd. utilizes escalation processes and defined responsibilities for addressing escalated matters. To escalate a Case, the Client may telephone or email the service desk (quoting the reference number).

Dependent on the escalation, NTT Ltd. may assign an Escalation Manager who is responsible for:

- Monitoring escalated matters through to resolution
- Creating and maintaining an action plan for each escalation
- Making any decision appropriate to the resolution of the escalation
- Arranging escalation meetings and/or phone conferences (as appropriate) between the Client, NTT Ltd. and relevant third parties
- Regularly communicating escalation status to:
  - The Client
  - The NTT Ltd. Client Services Manager (if assigned)
  - Any other parties relevant to the escalation

- Regularly updating and seeking the advice and support of NTT Ltd. management
- For the duration of an escalation, ensuring all appropriate personnel are available to support the agreed action plan

NTT Ltd. may downgrade an escalated Case if it is being managed to a scheduled timeframe, or resolution has been provided to the Client and is in the process of being tested. If the Client initiated the escalation, NTT Ltd. will obtain the Client's approval prior to downgrading an escalated Security Incident, Incident, Change Request or Service Request.

Clients may request their Case be escalated to a higher priority at any time if sufficient justification is provided. Upon review, the SOC manager shall be responsible for agreeing actions.

4 Service Transition

Service Transition is executed in five phases, these are:

1. Engagement
2. Planning
3. Staging
4. Integration
5. Go-Live

The five phases and activities and procedures within them, ensure a consistent approach to management and completion of the transition and a framework for governance and communication. During the first four phases of the Service Transition period there will be no alerts, incidents, or cases generated for customer review and triage.

4.1 Engagement Phase

To initiate the Service Transition, the Client will submit a Purchase Order (PO) along with the Pricing Information from the approved quotation, a High Level Design document, and the Client Security Services Detail to NTT Ltd.

- Purchase Order (PO) and
- Pricing Information
- Client Security Service Detail (CSSD)
- High Level Solution Design

NTT Ltd. reviews the provided documentation and confirms that all the requirements for commencement of the transition have been met.

A Kick-off meeting is held to communicate the Transition Process, the project tasks, roles and responsibilities and introduce the key stakeholders.

The Engagement Phase is expected to take 12 business days and can be accelerated if the Client provides completed and accurate documentation when submitting the Transition Service Request.

4.1.1 Engagement Phase Activities

The key activities during the Engagement Phase are as follows:

- Receive the Service Transition Request and PO and respond within three business days
- Review provided documentation within six business days
- Provide feedback and confirm content is complete and aligned to the Service Order
- Assign a Service Transition team including allocation of an NTT Ltd. Client Service Manager (CSM)
- Create the Draft Service Transition Project Plan, including timeline and constraints within 10 business days
- Arrange a Kick-off meeting within 12 business days (if documentation is complete and confirmed)

4.1.2 Engagement Phase Deliverables

The deliverables provided during the Engagement Phase are as follows:

- Purchase Order Approval
- Kick-off meeting (face to face or call)
- Draft Service Transition Project Plan, including timeline, standard risks and issues

4.2 Planning Phase

The Service Transition Planning Phase validates the provided documentation and locks down the transition plan, scope, and timeline. The Planning Phase is expected to take six business days.

4.2.1 Planning Phase Activities

The key activities during the Planning Phase are as follows:

- Agree on final architecture, including devices and logs collection
- Assess Log Source Scope and Prioritization, including completing Log Source Inventory where applicable
- Client Approval of Final Service Transition Plan
- Confirm Services Delivery Model, including Incident Management and Steady State Governance

4.2.2 Planning Phase Deliverables

The Final Service Transition Plan (including timeline, risks, and issues) is provided as a deliverable during the Planning Phase.

4.3 Staging Phase

The Service Transition Staging Phase establishes the primary service elements for NTT Ltd. to provide the service. It includes connectivity, appliances for log collection and device management access, and Portal and IT Service Management (ITSM) setup. The Staging Phase is expected to take 12 working days.

4.3.1 Staging Activities

The key activities during the Staging Phase are as follows:

- Install appliances (shipping, if required)
- Appliance initial configuration and hardening
- Setup and validation of remote access
- Log(s) events/ monitoring setup (Client device)
- OOB configuration (if applicable)
- MSS SOC Portal account(s) configuration
- MSS SOC infrastructure preparation

4.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

- Appliance required to support Client services
- Client credentials for MSS Portal
- Client Entitlement in NTT Ltd. ITSM
- Test results

4.4 Integration Phase

The Service Transition Integration Phase completes the required technical service elements for NTT Ltd. to provide the service. It includes configuration of all purchased services, advanced features for log collection (if applicable) and device management, and final Portal and ITSM integration. Additionally, during the Integration Phase, the NTT Ltd. CSM conducts the Welcome meeting and Portal training with the Client.
The Integration Phase is expected to take 21 business days.

Following the Welcome meeting, the CSM becomes the interface into the our services.

4.4.1 Integration Activities

The key activities during the Integration Phase are as follows:

- Final validation of connectivity to the SOC
- Device(s), log(s), and service testing and final verification
- Normalization and tuning (logs, not devices)
- Quality assurance review and activation of the service(s)
- Risk and Issue documentation
- MSS SOC Welcome meeting or call with Partners and Client (NTT Ltd. decision)
- MSS SOC Portal training meeting or call with Partners and Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and SLA start date

4.4.2 Integration Deliverables

The deliverables provided during the Integration Phase are as follows:

- Client Welcome meeting and Portal training
- Service Activation Date
- Confirmation of Device Management Readiness
- Client review and acceptance of the Risk and Issue Register

4.5 Go-Live Phase

The Service Transition Go-Live confirms that the service is live and closes the Service Transition Project. The Go-Live Phase is expected to take six working days.

4.5.1 Go-Live Activities

The key activities during the Go-Live Phase are as follows:

- Operational Check List review by SOC
- Conduct Service Transition Plan closure review meeting or call with Partners and Client (NTT Ltd. decision)
- Review all remaining open action items including lessons and risks/issues to be considered for Steady State (going forward)
- Receive Client Service Transition Plan closeout final approval

4.5.2 Go-Live Deliverables

The deliverables provided during the Go-Live Phase are as follows:

- Risks/Issues Register (if any)
- Commencement of service and Billing
- Lessons learnt (if any)

4.6 Service Transition Deliverable Acceptance

The Service Transition is considered complete on the Service Activation Date and after any Go-Live deliverables are provided. The deliverables are considered as being accepted at the completion of next phase. The Client will close the Service Transition by agreeing to the closure of the parent ticket in ServiceNow.

5 Device Management Features

Device Management Enhanced provides a 24/7 fully managed service including health and availability, backup and restore, release management and full change management. NTT Ltd. provide flexibility through optional co-management where a Client can maintain control and access to their security infrastructure if required.

This section presents the features of the Device Management Enhanced service.

5.1 Health and Availability Monitoring

5.1.1 Health and Availability Monitoring

The Device Management (Enhanced) Service monitors key performance indicators of in-scope configuration item's service state and resource utilization to determine overall health, performance and availability. The service automatically generates Incidents in the ITSM system based on events which exceed thresholds against specific poll cycles of key metrics. Events are investigated and analysed by a SOC engineer who determines a potential corrective or control action to resolve the related Incident as defined within Section 5.2. The Client will be notified and kept up to date of issues with overall health and availability via the Incident ticket available on the NTT Portal.

5.1.2 Health and Availability Improvement and Recommendation

NTT Ltd. utilize standard poll cycles and thresholds when monitoring in-scope configuration items. NTT Ltd. may adjust thresholds based on historical data collected to eliminate unnecessary events occurring. With this data, NTT Ltd. may identify potential methods of improving configuration item performance and overall health and availability. A Client can also request customization of thresholds through standard change management processes.

5.1.3 Health and Availability change implementation

If changes to a configuration item are required, NTT Ltd. will follow the standard Change Management process outlined in Section 5.5.3.

5.2 Incident Management

Incident Management focuses on responding to any unplanned interruption to service and configuration item operation to minimize any impact to business operations and ensure service quality and availability.

5.2.1 Incident Generation

Incidents may be generated through Health and Availability Monitoring, by the SOC or Client raising an Incident Case via the NTT Portal or telephone call to the SOC.

For an Incident Case raised via the NTT Portal, with a provided Impact and Urgency, the SOC team will validate the ticket and reserves the right to modify the Impact and Urgency as deemed necessary.

For an Incident Case raised via a telephone call to the SOC, the SOC shall create an Incident Case on behalf of the Client with the relevant Impact and Urgency.

5.2.2 Incident Diagnosis

Incident Cases are managed based on the priority of the Incident ticket raised on the NTT Portal. Priorities are calculated based on Impact and Urgency of an Incident Case, leading to a specific priority. Priorities are defined as Major, High, Moderate and Low as outlined in the table below.

Impact
1. Organization wide
2. Multiple Departments
3. Single Department
4. Individual

Urgency
1. Work blocked
2. Work degraded
3. Work not affected

		Urgency		
		1	2	3
Impact	1	Major=P1	Major=P1	High=P2
	2	Major=P1	High=P2	Moderate=P3
	3	High=P2	Moderate=P3	Low=P4
	4	Moderate=P3	Low=P4	Low=P4

The SOC will triage the Incident to assess the priority. Incidents will be assigned to the appropriate SOC engineer who will investigate and analyse further to identify a correction plan to resolve the Incident Case. Clients are notified of updates to an Incident via the NTT Portal and any restoration plan to resolve.

5.2.3 Incident Resolution

We will work to resolve incidents and move to a 'resolved' state to allow customers to confirm resolution. Incidents will then remain in a resolved state until:

- Client confirms resolution and the incident will be moved to a 'closed' state
- Client confirms incident is not resolved, the ticket will be moved back to a 'In Progress' state
- Client does not respond, and the incident will be auto closed after 10 days.

We will keep Clients updated on any Incident resolution plans via the NTT Portal. Resolution targets are outlined in the Device Management Operational Level Agreement.

5.2.4 Incident Reporting

Clients are notified of all Incidents via a notification email which contains very minimal information for security purposes, with the full Incident details only available via the NTT Portal.

5.3 Capacity Management

5.3.1 Capacity monitoring and reporting

The monitoring systems utilized within the Device Management service regularly check a number of telemetry points. Through continuous monitoring, NTT Ltd. is able to highlight potentially impacting trends. This can be useful for determining if there is a problem that needs to be addressed or if configuration items are becoming oversubscribed, eg. a disk filling with log data. Using this as a starting point for Incident or Problem Management, NTT Ltd. will work with Clients to either resolve or mitigate the risk.

We utilize standard thresholds when gathering monitoring data, acknowledging that these thresholds may not be applicable to some Client environments, we can work with the Client to adjust thresholds during the Service Transition process or after service go-live where a baseline can be identified. If thresholds are changed, the Client must accept that this may result in unnecessary events or even false positives and we reserve the right to adjust thresholds accordingly.

5.3.2 Capacity improvement recommendation

Where NTT Ltd. monitoring determines a device is oversubscribed, we shall liaise with the Client to determine the best plan and path forwards. Examples include but are not limited to the following: Request for Change to logging levels or to network architecture; Request for Change to stated monitoring levels within the configuration item (for example turning off debug logging); Request for new hardware or licenses to facilitate greater capacity.

5.3.3 Capacity Planning

With the aforementioned trend data available, NTT Ltd., Partners and/or Clients may make decisions about future requirements and expected growth. This provides invaluable forward planning to those responsible for budgeting or capacity planning. For example, trend analysis reports will show disk consumption over time which could be an indicator of a need to procure new hardware or additional storage in the next budgeting cycle.

5.3.4 Capacity Change Implementation

Through the consistent and uniform measurement of telemetry from managed security configuration items, NTT Ltd. can make recommendations or raise a Request for Change Case to be approved by the Client to enhance or avoid future capacity issues that might arise. (Subject to the necessary approvals and advice being followed). Any capacity issues related to hardware refresh or design are not in scope.

5.4 Asset Tracking and Reporting

5.4.1 Configuration Item Recording

NTT Ltd. record and track in-scope Client configuration items with information available within the NTT Portal.

5.4.2 Configuration Item Control and Updates

5.4.2.1 Patch and Security Hotfix

NTT Ltd. monitors Original Equipment Manufacturer (OEM) published patch, security hotfix and version updates associated with in-scope configuration items and reviews such releases for applicability. If we determine such updates or patches are recommended for security or operational reasons, we will request approval prior to implementing any such updates through an NTT Ltd. sourced Change Case.
See Section 5.5.3.2.

NTT Ltd. will install an unlimited number of qualified and applicable software patches and OS minor version upgrades for in-scope configuration items. All patches or minor version upgrades are considered Normal Changes, therefore, all applicable Change Management processes apply.

If we determine a Client's in-scope configuration item is susceptible to a new vulnerability, classified as Low or Medium, NTT Ltd. will seek Client approval, prior to taking any response steps. In the event a SOC Engineer deems a new vulnerability classified as High in severity, we may take immediate response steps through an Emergency Change Case.

5.4.2.2 Major Version Upgrades

Major version upgrades require careful planning, coordination, management and roll back planning. NTT Ltd. considers all major version upgrades as high risk as they pertain to Client Production environments. With this in mind, major version upgrades are considered Project Orientated Requests (PORs).

NTT Ltd. will coordinate all major version upgrades with the Client and may agree to utilize the SOC and MACD service units, propose a fixed price project or perform the work on a time and materials basis.

5.4.2.3 Signatures

5.4.2.3.1 Updates

Where applicable, configuration item signature databases are usually automated and require connectivity between the configuration item and the internet to download the updates. NTT Ltd. checks that signature updates are being updated successfully.

5.4.2.3.2 Failures

If the signature update fails, an Incident is raised on behalf of the Client. Subsequently, any errors related to a configuration item's ability to update signatures is resolved using the standard Incident management process.

5.4.2.3.3 Escalations

If the cause of the configuration item's inability to update signatures is an error or deficiency in the manufacturer's database, NTT Ltd. shall escalate the issue to the manufacturer on the Client's behalf.

5.4.2.3.4 Client responsibilities

The Client is responsible for compatibility, user acceptance testing and functional testing within the Client's production environment. The Client ensures all configuration items are connected to the internet to enable delivery of automated signature updates from the configuration item manufacturer, either directly, through a proxy or through a dedicated management system.

5.4.2.3.5 Implied service level agreement

If the failure of signature update mechanism is diagnosed as a manufacturer related Incident, the service level to resolve the Incident will be in accordance with that manufacturer third-party supplier agreement.

5.4.3 Configuration Item Backup

NTT Ltd. maintains a backup of in-scope configuration item system and configuration(s) in case of failure or where applicable unless otherwise noted as the Clients responsibility.

NTT Ltd. shall backup the whole configuration item system every 24 hours which may be utilized for restoration in the case of a disaster recovery scenario. NTT Ltd. retains a maximum of 7 (seven) previous full system configuration item backups which are stored within the MSS infrastructure.

Where we are unable to obtain a new backup from the configuration item, the last successful backup will be stored. We will retain the last successful backup for 1 (one) year.

NTT Ltd. shall take a configuration backup before a Request for Change is implemented and utilize the backup to roll back to the last known configuration in the event of a failure or request by the Client.

We backup the following configuration item information (where applicable):

- System configuration (operating system and configuration)
- Configuration rules
- Signature configuration
- Signature pack
- Configuration files
- User database
- Operating system configuration
- Management device configuration

The scope of backup may differ from device-to-device based on manufacturer files and configuration.

5.4.4 Configuration Item Restore + OOB

Remote Management Kit (RMK) provides Out of Band (OOB) Management of in-scope configuration items – it is not applicable or supported for virtual or cloud based configuration items.

OOB access is utilized if in-scope configuration items encounter a catastrophic failure or connectivity to the Client infrastructure is lost requiring remote troubleshooting and maintenance activities. The RMK is under complete control by NTT Ltd. who will maintain the equipment hardware and software.

As such, the Client:

- Must not direct any unauthorised traffic to the RMK device
- Must not attempt to login to the RMK
- Must not tamper with the RMK
- Must not attempt to perform any penetration test without express written consent from NTT Ltd.

Should both the primary and OOB solutions become inoperable or otherwise unavailable for use by NTT Ltd., we reserve the right to suspend Services for the applicable configuration items until the situation is remedied. NTT Ltd. is not responsible for any Incident involving an in-scope configuration item while connectivity to the RMK is unavailable.

Through the RMK, NTT Ltd. provide restoration of backups to in-scope configuration item(s) in the event of a failure or if roll back to a previous configuration is desired provided that the NTT Appliance has the relevant connectivity and can push a restore operation to the in-scope configuration item(s).

The RMK's are monitored as part of the managed service.

5.4.5 Configuration Item Status Reporting

Configuration item status reporting is available via the NTT Portal. Status reports include version details and traffic light status.

5.4.6 Co-Management

Co-Management is a chargeable option which must be purchased to be enabled. In a co-managed scenario, specific conditions apply as outlined below:

- Co-management is only available as an option within the Enhanced service offering
- Configuration item availability (Service Level Target) is not applicable
- Configuration item configuration and policy changes can only be made by specific contacts by raising a Case via the NTT Portal
- Access to devices must be defined from specific Client internal locations/workstations (i.e. IPs/subnets)
- For NTT Ltd. to provide effective support the Client shall:
  - Notify NTT Ltd. in advance of changes being made to include scheduling and scope of changes being made to avoid 'lost transaction' or collision of change work
  - Record all modifications to be made via a Case within the NTT Portal
  - Explicitly request a backup via a Case on the NTT Portal
  - If applicable and upon completion the Client shall provide a report/status update from their internal Change Management process to ensure NTT Ltd. is aware of all the changes occurring to configuration item(s)
  - The Client shall make changes to configuration item such that there is a clear audit trail indicating the party responsible for the change, the date of the change and customer change control identification
  - Each change must be made in such a way as to provide the possibility of rolling back to the previous version. Failure to do this may render it impossible to recover the rule base if problems occur
- Any changes to NTT Ltd.'s service administration rules must be agreed by NTT Ltd. in writing by means of a Case prior to their implementation.

Clients accept any exception that may arise due to deviation from, or circumventing the processes described may result in an unsecured device(s) and/or non-compliant configuration(s) and, accordingly, Clients release NTT Ltd. from any liability resulting from outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to changes implemented directly by Clients. NTT Ltd. may, at its discretion, roll back to the previously available backup and will not be responsible for any previous changes lost or loss of service as a result.

5.5 Service Request Fulfilment

Service Request Fulfilment focuses on request for information, advice or access.

5.5.1 Service Request Management

Service requests are managed through ITIL process and raised via a Case in the NTT Portal. Attainment of various key performance metrics are tracked, monitored and reported within NTT Ltd. on a monthly basis.

5.5.1.1 Request for Information

Clients may request information through the NTT Portal about the performance, configuration or other aspects of in-scope configuration items. NTT Ltd. shall deduct the commensurate number of MACD units (if applicable) and provide the information in the Service Request.

5.5.1.2 Service Request Reporting

All Incidents, Service Requests, Problems or Changes are recorded in the ITSM system and reported back through the NTT Portal.

5.5.1.3 Project Oriented Requests

NTT Ltd. will charge, and the Client agrees to pay, the then-current applicable hourly rates for work associated with PORs. If any Change performed by the Client results in adverse effects and requires remediation work be performed by NTT Ltd. to restore the software/configuration item to proper working service, the Client agrees to pay NTT Ltd. the then-current Engineering hourly rate to return the 'in-scope' device to normal operating run-state.

5.5.2 Move, Add, Change, Delete (MACD) Fulfilment

Change Requests are administered through a Move, Add, Change, Delete (MACD) service unit model and are requested via the NTT Portal as outlined within Change Management.

MACD service units are bundled within the Enhanced service offering with option to purchase additional MACD units and are based on configuration item sizing. MACD's are deducted in the execution of any Client sourced service requests pertaining to Request for Changes of configuration items. The number of MACD service units deducted per service request is based on a predefined list of standard tasks that NTT Ltd. has derived assessing level of complexity to route accordingly to an appropriate SOC engineer.

The following table outlines the number of MACD's bundled per device, annually with the Device Management Enhanced service level:

Size	MACD Service Units
Small	25
Medium	30
Large	40
xLarge	50

MACD service units are aggregated across the total number of in scope configuration items and can be utilized across any device.

The MACD Service Unit Usage Tables per technology documentation is available upon request.

Where the usage of MACD service units for a service request exceeds 6 hours of effort, NTT Ltd. may charge additional MACD service units or propose a Project Orientated Request (POR) to perform the work on a time and materials basis.

MACD unit usage is tracked by NTT Ltd. and is included within any scheduled service reviews to ensure the Client account is operating in line with MACD availability. Should MACD unit balance drop below a certain threshold the Client will be notified for purchase of additional MACD service units.

5.5.2.1 Non-Standard Tasks Utilizing MACD Service Units

In the unlikely event that there is not a pre-existing menu item for a Client request, NTT Ltd. considers this a non-standard task.

NTT Ltd. will review non-standard tasks requested by the Client to determine if:

- NTT Ltd. has the appropriate skills to action or implement the task
- Whether the non-standard task should become a standard task (based on demand/repeatability)

NTT Ltd. will assess the non-standard task to determine the correct number of MACDs. NTT Ltd. will provide the Client with the number of MACD service units the task will incur for approval to proceed. Once approved by the Client, NTT Ltd. will execute the Request for a non-standard pre-approved task. No service levels will apply to the execution of a non-standard task.

5.5.3 Change Management

At a Client's request, NTT Ltd. will implement a request for change to in-scope configuration items in accordance to an associated MACD task or Non-Standard task outlined in section 5.5.2.1

NTT Ltd. provide specific Operational Level Agreements for Request for Changes which can be found in the Device Management Operational Level Agreements.

5.5.3.1 Client-sourced requests

Request for Change Cases must be submitted by valid Client contacts within the NTT Portal.

5.5.3.2 NTT Ltd.-Sourced Requests

NTT Ltd. may submit a Request for Change Case when a correct control change is necessary to resolve a Problem or Incident.

5.5.3.3 Change Reporting

All Changes must be reported and tracked via the NTT Portal, this includes co-managed scenarios.

The party making a Change is required to open an applicable Request for Change Case in the NTT Portal prior to implementation to ensure coordination between both parties.

5.5.3.4 Request for Change

All requests for change types follow the NTT Change Management process and require approval by NTT Ltd. NTT Ltd. derive tasks per technology which corresponds to the number of Service Units utilized by each task. There are 3 (three) types of request for change outlined below.

Normal Change

Normal Changes require approval (from both NTT Ltd. and Client respectively) before being implemented. Neither Client nor NTT Ltd. is authorized to apply Changes on behalf of the other without documented consent from appropriately authorized individuals (documented within a Change Approver Group on the NTT Portal) from both parties via a Request for Change Case resident in the NTT Portal.

Standard Change

NTT Ltd. is authorized by the Client to apply Changes without authorization from the Client when a standard change ticket is raised via the NTT Portal, though an NTT Ltd. internal approval process is still valid.

Emergency Changes

An emergency change is considered a request for change that must be implemented as soon as possible, for example to resolve an Incident or implement a security patch. NTT Ltd. will work with the Client during the Change Management process.

Cancelling a Request for Change

The Client may cancel a Request up to 2 hours before any scheduled changes being committed to the device configuration. In which case any MACD credit that would have been deducted shall be cancelled.

If the Client would like to reverse a Change that has already been implemented, the Client must submit a new Service Request for Change via the NTT Portal. In which case the commensurate MACD credits shall be deducted for both the original change and any subsequent reversal requested.

5.5.3.5 Change Implementation

The party making the Change must complete and document the following tasks associated with each Change:

- Backup the current running configuration(s) prior to the change or if co-managed must notify NTT Ltd. to ensure a backup is taken
- Ensure a copy of any applicable software and/or firmware is readily accessible
- Ensure a roll back plan is documented in the event there are issues with the Change
- Assign an internal ticket number (if applicable) to track the Change for auditing purposes
- Implement and test the Change (as far as is possible – testing responsibility is also shared with the Client) to confirm whether the change met the requirements as specified by the submitter.
- Create a backup of the new configuration after the Change is implemented
- Update NTT Ltd.'s Service Request ticket indicating whether the Change was successful or not

It is imperative each Change is fully documented within the NTT Portal to ensure NTT Ltd. can quickly troubleshoot if/when unanticipated negative consequences arise.

Exceptions

The Client understands any exceptions that may arise due to deviation from or circumventing the processes described herein may result in unstable and/or unsecured configuration item(s) and/or non-compliant configuration(s) and accordingly, the Client releases NTT Ltd. from any liability resulting in outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to any Change made by the Client.

The Client agrees any work performed by NTT Ltd. to troubleshoot issues directly attributable to a Client Change is billable at the current NTT Ltd. Engineer's hourly rate.

Client Responsibilities

The Client agrees only appropriately-trained and skilled engineers will perform Changes in a co-managed environment.

The Client understands that NTT Ltd. reserves the right to bill for incremental troubleshooting work NTT Ltd. performs as a result of:

- Client not accurately recording changes on their in-scope configuration item(s)
- Client not notifying NTT Ltd. about changes being made with at least 1 full business day's notice
- Client performing work that violates OEM support agreements or leads to in-scope configuration items negatively effecting Client production environment

NTT Ltd. Responsibilities

NTT Ltd. will review Incident, service requests and documentation regarding changes performed by the Client and may seek clarification.

5.5.3.6 Change Impact Analysis

As part of the Change design process, NTT Ltd. conduct a Change Impact Analysis in accordance to all Requests for Change Cases (pre- and/or post-implementation). NTT Ltd. reviews Incident cases, service request cases and documentation regarding Requests for Change Cases in the event of a co-managed service and may seek clarification.

NTT Ltd. will conduct a Change Impact Analysis prior to implementation of any Request for Change Case – including request for change, Patch and Version Management, or PORs to ensure:

- Hardware/software meets all prerequisites
- Backups of previous version/configuration exists
- Any change is consistent with security best practices and does not compromise the Clients network, service or that of NTT Ltd.
- Any change is relevant to Client's environment
- Any change can be implemented within the requested timeframe

NTT Ltd. considers the Change Impact Analysis complete when Client has addressed all issues raised during the analysis (if applicable), and the engineer acknowledges receipt of a valid Request for Change via the NTT Portal.

5.6 Problem Management

5.6.1 Problem Identification and Recording

NTT Ltd. follow ITIL best practices for Problem identification and recording. Problem identification is performed in a number of ways and will typically result in a Problem Case in the NTT Ltd. ITSM tool and NTT Portal. Typically, Problems are derived from a number of factors such as:

- Repeated Incidents of same or similar nature within single Client or across multiple Clients
- Compound problems caused by multiple Incidents of different nature within single Client
- Notification of problem from Manufacturer
- Lack of timely patch from Manufacturer to address security vulnerability
- Trend analysis

5.6.2 Problem Reporting

All Problems are recorded in the ITSM system and reported back through the NTT Portal.

5.6.3 Solution Identification and recording

Once a problem is identified and recorded, a suggested plan or where appropriate a number of suggested options for resolution will be recorded in the problem ticket.

5.6.4 Solution Implementation

The Client and NTT Ltd. shall discuss and agree on the best or most appropriate solution and implement as a controlled change or series of changes in line with the standard change process.

6 Terminology and Definitions

Terminologies and Definitions for Security Device Management services are presented in the 'NTT Ltd. - Terminology and Shared Services Reference' document that accompanies this Service Description.

The unique definitions used within this Service Description are:

Case	A Case is a record used to identify and resolve various types of issues or requests – they are related to record types such as change requests, incidents and service requests.
Out of Band (OOB)	Access to a configuration item through a stream that is independent from the main in-band data stream
Problem	A cause of one or more Incidents

7 Operational Level Agreements

Operating Level Agreements for Security Device Management services are presented in the 'Operating Level Agreements – Managed Security Services' document that accompanies this Service Description.

8 Changes in Service

Operating Level Agreements for Security Device Management services are presented in the 'Operating Level Agreements –

8.1 Regulatory Change Requirements

If regulatory changes (e.g., changes by a regulatory agency, legislative body, or court of competent jurisdiction) require NTT Ltd. to modify the Services described herein, NTT Ltd. will modify the Services and this Service Description accordingly without diminishing the features, functionality or performance. In the event a modification in response to regulatory changes results in a diminishment of features, functionality or performance, Client agrees in good faith to work with NTT Ltd. to amend this Service Description accordingly and execute any additional agreement which may be reasonable requested by NTT Ltd. to document such amendment.

8.2 Method of Service Delivery

NTT Ltd. reserves the right to make changes to the service, provided these changes do not have a material adverse impact on functionality or performance.

8.3 Supported Devices

NTT Ltd. reserves the right to change Supported Device's over time as new manufacturer hardware models and software versions are released or announced by the manufacturer as End of Support and/or End of Life.

9 Service Exclusions

Unless otherwise expressly agreed by NTT Ltd. in writing, the services described in this document do not include the following:

- Configuration of in-scope security systems and devices to allow for Log, Events, and evidence collection.
- Support and Remedial Work which is not expressly stated in this Service Description This includes any troubleshooting and problem solving related to issues arising from Client actions or Client's network.
- Project Orientated Requests (PORs) are not included in the Services described herein and are subject to additional fees. NTT Ltd. and the Client will develop a scope for the POR and NTT Ltd. will provide a separate quote to Client, which must be executed prior to performance of any such work.
- Client requests for advice or consultation regarding network or configuration item configuration not specifically outlined in this Service Description is not included are subject to additional fees.
- Client staff training unrelated to NTT Ltd. services (NTT Ltd. provides written and video training on the NTT Portal and the different functions that Client may use within the portal.).
- Software or hardware maintenance (unless otherwise stated).
- Software licensing (unless otherwise stated).
- Software or hardware upgrades.
- Network connectivity troubleshooting.
- On-site forensic services.
- Security policy or procedure establishment.
- Firewall rule set design, validation and troubleshooting.
- Remediation of a Security Incident or attack on a Client's network, server or application.

10 Controlling Terms

In the event of any conflict between the terms of this Service Description and the terms of the Client agreements, the terms of this Service Description shall control.

NTT

Together we do great things