Client Service Description

Security Device Management Services

20 October 2020 | Document Version 1.8

NTT contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

FirstName LastName – Services Product Portfolio Director – Security, Phone: +1 203 446 4942

NTT Limited
✉ firstname.lastname@global.ntt

Please quote reference {Document Reference Number} in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of NTT Limited ('NTT'). {ClientFull} ('{Client}') may not disclose the confidential information contained herein to any third party without the written consent of NTT, save that {Client} may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of {Client}'s evaluation of the document. {Client} agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as {Client}. As a condition of receiving this document, {Client} agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

NTT and {Client} acknowledge and agree is subject to NTT's standard terms and conditions which are available on request. NTT reserves the right to vary the terms of this document in response to changes to the specifications or information made available by {Client}. Submission of this document by NTT in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

NTT does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with NTT will be governed by {Law} Law and be subject to the exclusive jurisdiction of the {Law} courts.

Document Preparation

	Name	Title	Date
Prepared:	Paul Asdagi	Service Director – Group Security	12 Sep 2018
Prepared	Mike Oberholtzer	Sr. Product Manager	01 Feb 2019
Prepared	Bob Gordon	Portfolio Director – Security	06 Jun 2019
Updated	Sharon Witheriff	Technical Writer	07 Jun 2019
Updated	Bob Gordon	Portfolio Director – Security	01 Oct 2019
Updated	Tore Terjesen	Director	13 May 2019
Updated	Tore Terjesen	Director	20 Oct 2020

Release

Version	Date Released	Pages	Remarks
1.3	06 Jun 2019		Internal DRAFT
1.4	07 Jul 2019		Internal DRAFT
1.5	01 Oct 2019		Rebrand
1.6	13 May 2020	All	Updated to reflect the latest Service Description
1.7	20 Oct 2020		Added SaaS Policy Mtg. support to DM-E
1.8	20 Nov 2020		SLA added

This document is only a general description of the available Services. The Services to be supplied are subject to change. For each Client, the Services will be as set out in the contract entered into by the Client and NTT. If there is any conflict between this document and the contract, the contract will prevail.

Table of Contents

List of Figures

List of Tables

1. Service Description

1.1. Overview

Getting the basics right from the start is a fundamental aspect to good cybersecurity practices. Secure configuration, management and maintenance of security devices are essential to protect those assets and meet numerous compliance regulations.

24/7 operational capabilities are costly especially when premium security skills are required for a multitude of technologies. Standardized and repeatable security operations can be addressed with a cost effective alternative, de-risked through ITIL and security best practice from NTT.

Our Security Device Management Services are extremely effective in reducing the day-to-day operational burden on overstretched IT staff allowing them to focus on more strategic challenges. Leveraging decades of security experience, we can comprehensively meet your security demands in line with your overall business requirements, at a predictable cost.

We provide operational excellence through a network of NTT Security Operations Centres (SOCs) strategically located around the globe with ISO27001 certification, enabling a consistent and reliable security program.

We follow Information Technology Infrastructure Library (ITIL) best practice, a process-based framework for repeatable and consistent service delivery. Specifically, for the Security Device Management Services, we follow ITIL best practice for service operation with all NTT Managed Security Services encompassed by our company wide Continual Service Improvement process. Key operational processes link together to provide an effective overall support structure with distinct processes aligned to our SOCs and service tools.

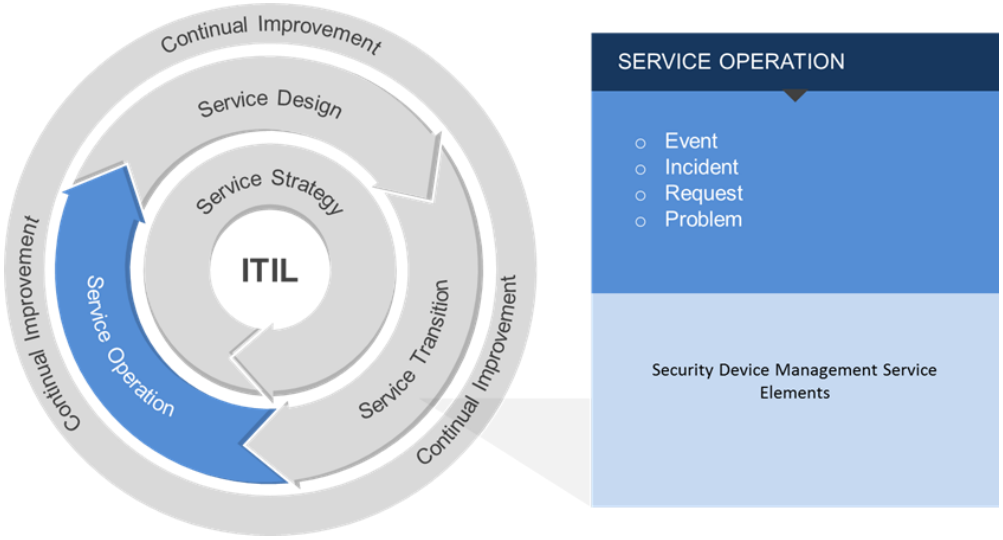

Figure 1 Service Operation

Security Device Management Services come in two Service variants - Standard and Enhanced.

Security Device Management – Standard provides 24/7 health and availability (H&A) monitoring of devices notifying you of any H&A related incidents which may cause disruption to your business. In this service offering you maintain complete control of your security infrastructure but leverage our 24/7 SOC capabilities for monitoring only.

Security Device Management – Enhanced builds on the Standard Service variant to offer a 24/7 managed service including H&A, backup and restore, release management and full change management. We provide flexibility through optional co-managed services where you can maintain complete control and access to your security infrastructure, if required.

Specific to supported Third Party Software as a Service (SaaS) applications Device Management - Enhanced includes policy management via the change management process with predefined move, add, change, and delete (MACD) bundles.

Security Device Management Services provide:

- on-demand device configuration and tuning
- timely updates and patch management
- continuous device H&A monitoring
- 24/7 coverage via our ISO/IEC 27001-certified SOCs
- highly experienced and certified industry and vendor experts
- proven operational processes aligned with industry best practice and guidelines
- device incident/event/capacity management and escalation through to resolution
- service level agreements, objective commitments, and targets.

Key Benefits

- Lower total cost of ownership (TCO) by leveraging our scale, processes, platform automation, and delivery model to manage your environment
- Integrated approach to the management of your security devices into one secure and reliably managed security device service
- Predictable costs
- Improved operational performance by leveraging our technical expertise, intellectual property, and best practices
- Mitigated risk of the transfer of operational control by having an integrated approach from sales, to service transition, to day-to-day operations

1.2. Service Matrix

The Security Device Management Services are available in two distinct Service variants.

The service variant, selected options and associated service levels forms part of your Managed Services Agreement.

Service Features	Service Variant	
	Standard	Enhanced
Core Service Features		
• Hours of Operation (24/7) • Security Operations Centres (SOCs) • Client Portal • Language Support • Management of Devices • Monitoring • Engineering • Security Appliance	✓	✓
Security Device Management Service Features		
Health and Availability Monitoring		
Health and Availability Monitoring	✓	✓
Health and Availability Improvement and Recommendation	✓	✓
Health and Availability Change Implementation		✓
Incident Management		
Incident Generation	✓	✓
Incident Diagnosis	✓	✓
Incident Resolution		✓
Incident Reporting	✓	✓
Capacity Management		
Capacity Monitoring and Reporting	✓	✓
Capacity Improvement Recommendation	✓	✓
Capacity Planning	✓	✓
Capacity Change Implementation		✓
Asset Tracking and Reporting		
Configuration Item Recording	✓	✓
Configuration Item Control and Updates		✓
Configuration Item Backup		✓
Configuration Item Restore + OOB		✓
Configuration Item Status Reporting	✓	✓
Configuration Management		
Service Request Fulfilment	✓	✓
Service Request Management	✓	✓

Service Features	Service Variant	
	Standard	Enhanced
Policy Management		✓
Move, Add, Change, Delete (MACD) Fulfilment		✓
Change Management		✓
Service Options		
Co-Management		✓
Service Management		
Service Level Management	✓	✓
Service Desk	✓	✓
Service Delivery Manager (SDM)	✓	✓
MSS Technical Account Manager (option)	✓	✓
Service Transition		
Client Transition	✓	✓

Table 1 Service Matrix

1.3. Supported Device Categories

NTT's Security Device Management Service supports your devices in the cloud and on premise. The following table lists supported devices by category:

NGFW/Firewall	Proxy	IDS/IPS	Sandbox
End Point (EDR)	Web Application FW	SSL VPN	
Mtg. consoles	Email GW	OT IDS Mtg.	

Figure 2 Supported Device Categories

1.4. NTT's Managed Security Services Portfolio

Figure 3 MSS Service Menu

2. Core Service Feature Descriptions

2.1. Hours of Operation

Security Device Management Services are delivered through our Security Operation Centres (SOCs), which operate 24 hours a day, 7 days a week.

2.2. Security Operations Centres (SOCs)

We will deliver Security Device Management Services from any of our SOCs at our sole discretion. Your data may be stored in any of the SOCs and on our global infrastructure unless there is prior agreement and approval between NTT and you.

2.3. Client Portal

You will have access to our Manage Centre Portal which is a globally available, web-based application which allows you to interact with, manage, and monitor your Managed Security Service.

2.4. Language Support

Security Device Management Services are provided in the English language only, unless there is prior agreement and approval between NTT and you.

2.5. Management of Devices (Enhanced Only)

Management of devices is included within the Security Device Management Enhanced Service variant with responsibilities dependent on the type of management services selected by you.

NTT offers two types of management:

- Standard Management (default)
- Co-Management

The management type of the Service is selected by the Client during the sales phase.

2.5.1 Standard Management

Standard Management is included as a core component of the Security Device Management Enhanced Service variant where you provide us with privileged access to configuration items within scope. You do not have any access to configuration items within scope unless the Co-Management Add-On is purchased or read-only access is requested. Standard management includes the following features:

2.5.1.1 Asset Management

- Control and Updates
- Backup
- Restore

Note. Asset Management does not apply to Third Party SaaS.

2.5.1.2 Configuration Management

- Ruleset and/or policy management

We will create one administrator account (Break Glass account) for you and will securely store the credentials and password. In the event of an emergency where we are unable to make a change or access the configuration item/management infrastructure, your primary security contact will be provided with the credentials and password.

Each time you use the Break Glass account, we reset the account with a new password.

Except with co-managed configuration items, you agree not to create any administrator or other change-capable accounts (i.e. “super user”) on “in-scope” configuration items. If required, you must request creation of such administrator accounts via Manage Centre. We perform periodic and ongoing auditing of all administrator accounts.

2.5.2 Co-Management

Co-Management is a chargeable add-on to the Security Device Management Enhanced Service variant. NTT and you and/or your nominated third party and/or an NTT Group Operating Company have access to configuration items with the ability to make updates and configuration changes. In a co-managed scenario, specific conditions apply as described in *4.1.1 Co-Management (Option for Enhanced Only)*.

2.5.3 Read Only Access

You can be provided with read-only access to configuration items.

2.6. Monitoring

2.6.1 Protocols

Your configuration items are monitored utilizing multiple protocols, including Simple Network Management Protocol (SNMP) v2, v3; Secure Shell (SSH) v2; Hypertext Transfer Protocol (HTTP); Hypertext Transfer Protocol Secure (HTTPS); and Internet Control Message Protocol (ICMP). For Third Party Supported SaaS applications this is not applicable.

2.6.2 Health and Availability Monitoring Events

The event feeds from in-scope configuration items are sent to the Security Appliance and securely sent to the monitoring server via a VPN in the MSS infrastructure. Note. Not applicable for Third Party SaaS supported applications.

2.7. Engineering

2.7.1 Configuration Item Access

Command-line access is secured via SSH v2. A trusted NTT jump host within the MSS infrastructure that leverages the Virtual Private Network (VPN) established

from NTTSA provides SSH access. Note. Not applicable for Third Party SaaS supported applications.

2.7.2 Application Access

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

Third Party SaaS applications are accessed via the public Internet leveraging the vendors chosen security protocols.

2.7.3 Backup (Enhanced Only)

Our MSS infrastructure contains a backup server and communication is secured over the VPN to the in-scope configuration item(s). The backup server is utilized to take backups of the in-scope configuration item(s), and is encrypted and stored within the MSS infrastructure.

For Third Party SaaS applications we will (where applicable) leverage the Third-Party SaaS applications backup features. Otherwise, backup does not apply for Third-Party SaaS applications.

2.7.4 Out of Band (Enhanced Only)

Out of Band access is provided for lights-out management of configuration items or in the event of an availability-affecting event such as a network outage. Out of Band access can be used to facilitate a bare metal restore of configuration items 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.

2.8. Security Appliance

NTT's Managed Security Services require a Security Appliance for most supported environments and technologies. However, NTT-supported Third Party SaaS applications can be supported without the Security Appliance.

Where SaaS applications have no Security Appliance dependency, access to SaaS applications will be facilitated directly via the Internet when deemed suitable by us.

The Security Appliance is available in multiple form factors, including a virtual image and physical appliance. You must install, initially configure and enrol Security Appliances. We 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 us.

Security Appliances gather log feeds and evidence data from your in-scope devices and systems then prepare the data for secure transmission and processing. Ongoing configuration and maintenance of the Security Appliance is conducted by us. Therefore, the Security Appliance should be installed by you in a suitable location on your network infrastructure to facilitate both access and log collection.

Key features of the Security Appliance include:

- physical or virtual form factors
- public cloud support
- the Security Appliances run on a hardened Linux operating system, fully maintained by us
- log and data capture with compression and secure forwarding to the NTT data centre
- encrypted connections to and from the NTT data center (zero touch ‘phone home’ VPN)
- custom developed networking to address multi-tenant address space issues
- secure access for backup and restore of your devices under management
- health and availability monitoring of your devices under management
- centralized management and configuration

The Security Appliance requires:

- two static (non-dynamic) IP addresses
- permanent LAN connectivity
- permanent Internet connectivity on TCP port 443

For the virtual form factor, the Security 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 us

3. Detailed Service Feature Descriptions

This section presents the features of the Security Device Management Services. Some of the features are only applicable to the Enhanced Service variant as we do not have access to your devices in the Security Device Management Standard Service variant. Enhanced-only service elements are called out specifically. See *Table 1 Service Matrix* for an overview.

3.1. Service Portal and Reporting

3.1.1 Manage Centre Portal

As part of any Managed Security Service from NTT, you are provided with access to NTT's Manage Centre Portal. Manage Centre provides online access to:

- interact with us online by logging incidents, requests and changes
- track, view and submit comments within incident, request, and change tickets
- view contract data
- browse and search our knowledge base, and
- access the online document repository for contractual documentation, procedural documentation, meeting minutes, etc.

Ticket level reporting is provided via a mixture of interactive dashboards, charts and downloadable reports. Through Manage Centre, you can:

- view summaries and drill down into the detail for analysis
- focus in on specific time periods
- export the underlying data for offline analysis or reformatting

Figure 4 Manage Centre Dashboards and Reports

3.1.2 Security Tools

For Security Device Management Services, you are provided with a set of Manage Centre Security tools:

- health and availability overview dashboards (traffic lights)
- assets overview
- availability overview

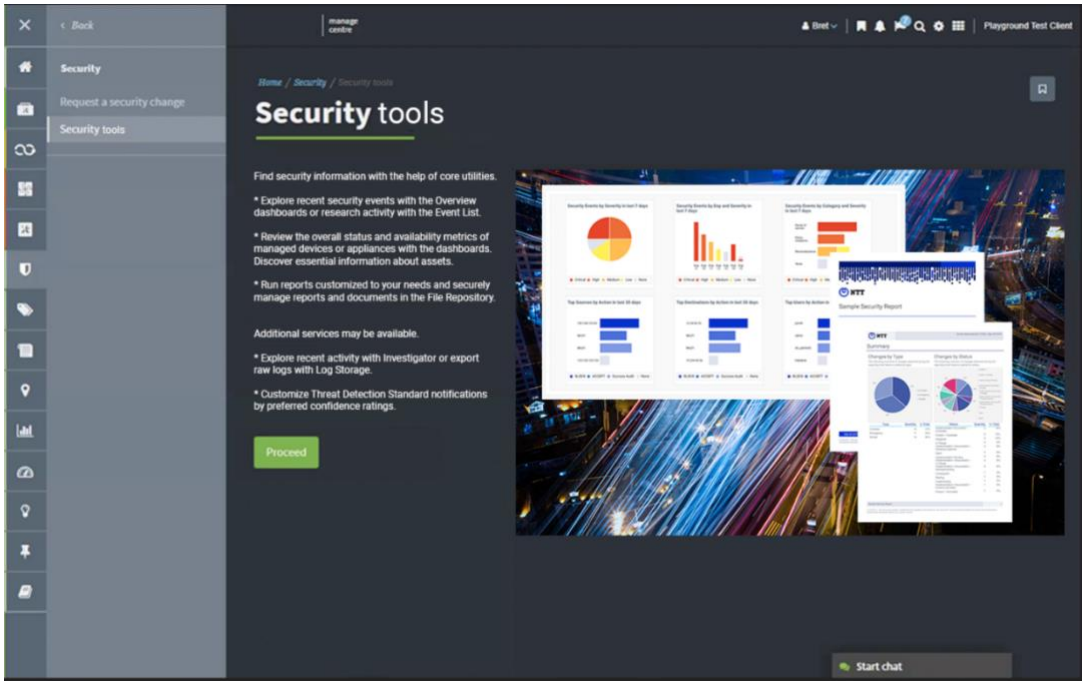

Figure 5 Manage Centre Security tools

3.2. Health and Availability Monitoring

3.2.1 Health and Availability Monitoring

Security Device Management Services monitor key performance indicators of a configuration item's service state and resource utilization to determine health, performance, and availability. The Services automatically generate incidents in NTT's 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. You will be notified and kept up to date of issues with health and availability via the incident ticket available in Manage Centre.

3.2.2 Health and Availability Improvements and Recommendations

We utilize standard poll cycles and thresholds to baseline configuration items. As a baseline is identified, we may adjust thresholds based on historical data collected to eliminate unnecessary events occurring. With this data, we may identify potential methods of improving configuration item performance and health and availability.

For the Security Device Management Enhanced Service variant, you can also request customization of thresholds through standard change management processes.

For the Security Device Management Standard Service variant (where we do not have access to make changes), if we make recommendations to you which have not been implemented and in-scope configuration items create unacceptable levels of events and/or incidents (assessed by us), we reserve the right to disable health and availability monitoring until recommendations have been actioned.

3.2.3 Health and Availability Change implementation (Enhanced Only)

If changes to a configuration item are required we will follow the standard change management process.

3.2.4 Third Party Software as a Service (SaaS)

You are responsible for the health and availability of your Internet connection and third-party services/applications. Note. NTT is not responsible for health and availability of Third-Party SaaS supported applications.

3.3. Incident Management

Incident management is the process for managing the lifecycle of an incident. The aim is to restore the Security Device Management Services as quickly as possible to minimize business impact. This is achieved through a temporary workaround or permanent fix, within the service level targets.

As part of the Security Device Management Services, we proactively identify incidents on configuration items.

The incident management process includes notification, status update, and escalation procedures that are executed by our SOC teams on a 24/7 basis. We manage incidents according to their assigned priority as outlined in 3.3.2 Incident Diagnosis.

3.3.1 Incident Generation

Incidents may be generated by the health and availability monitoring service, the SOC, or by you raising an incident-related ticket via Manage Centre or a telephone call to the Service Desk.

For incident tickets raised via Manage Centre, with impact and urgency provided, the SOC team will validate the ticket and reserve the right to modify the priority as deemed necessary.

For incidents raised by you via a telephone call to the Service Desk, the Service Desk will create an incident ticket on your behalf with the priority assigned based on the relevant impact and urgency.

For any urgent service disruption, we will advise you to open a case in Manage Centre and follow up with a call to the Service Desk using the ticket number.

3.3.2 Incident Diagnosis

Incidents are managed based on the priority of the incident ticket raised. Priorities are calculated based on the impact and urgency of an incident ticket. Priorities are defined as major, high, moderate and low.

		Urgency		
		1. Work Blocked	2. Work Degraded	3. Work Not affected
Impact	1. Organisation wide	Major	Major	High
	2. Multiple departments	Major	High	Moderate
	3. Single department	High	Moderate	Low
	4. Individual	Moderate	Low	Low

Table 2 Impact-Urgency matrix

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. You will be notified of updates to an incident via Manage Centre.

3.3.3 Incident Resolution (Enhanced Only)

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

- you confirm resolution - the incident will be moved to a ‘Closed’ state
- you confirm incident as not resolved - the ticket will be moved back to an ‘In Progress’ state
- you do not respond - the incident will be automatically closed after 10 days

Any ticket for an incident or request in a ‘Waiting’ state with a ‘Waiting on Customer’ reason which has no updates for 5 days will automatically move to a ‘Resolved’ state. Then will move to ‘Closed’ state automatically after 10 days.

Updates which restart the 5 day clock are updates such as additional comments being added to the ticket. A change in state on the ticket will cancel this functionality.

Within the Security Device Management Standard Service variant, we do not have the ability to resolve incidents due to not having administrative privileges to configuration items. Therefore, we will work on a best effort basis to advise you on the potential actions to resolve the incident. You are responsible for the resolution of the incident and must update any incident case(s) within Manage Centre to a resolved state to allow you to confirm resolution. Incidents will then remain in a resolved state until you:

- confirm resolution - the incident will be moved to a ‘Closed’ state
- confirm that the incident is not resolved - the ticket will be moved back to an ‘In Progress’ state (to be actioned by you)
- do not respond - the incident will be automatically closed after 10 days.

3.3.4 Incident Reporting

You will be notified of all incidents via a notification email containing minimal information for security purposes, with the full incident details only available via Manage Centre.

3.4. Capacity Management

3.4.1 Capacity Monitoring and Reporting

The monitoring systems utilized within the Security Device Management Services regularly check a number of telemetry points. Through continuous monitoring, we are able to highlight potentially impacting trends. This can be useful for determining if there is a problem that needs to be addressed or if the configuration items are becoming oversubscribed, for example, a disk filling with log data. Using this as the starting point of an incident, we will work with you to advise on a potential resolution or mitigate the risk.

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

Note. NTT is not responsible for capacity management of Third-Party SaaS applications.

3.4.2 Capacity Improvement Recommendation

Where our monitoring determines a device is oversubscribed, we will work with you to determine the best plan and path forward. Examples include but are not limited to:

- request you to change the logging levels or to network architecture
- request you to change the monitoring levels within the configuration item (for example turning off debug logging)
- request you to update hardware or licenses to facilitate greater capacity.

3.4.3 Capacity Planning

With the aforementioned trend data available, NTT, our partners, and/or you 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 the need to procure new hardware or additional storage in the next budgeting cycle.

3.4.4 Capacity Change Implementation (Enhanced only)

Through the consistent and uniform measurement of telemetry from managed security configuration items, we can make recommendations or raise a Request for Change (RFC) to be approved by you to enhance or avoid future capacity issues that might arise. This is subject to the necessary approvals and the advice being followed. Note. Any capacity issues related to hardware refresh or design are not in the scope of this Service.

3.5. Asset Management

Asset management is not applicable for SaaS supported applications.

3.5.1 Configuration Item Recording

We will record and track your configuration items with information available within Manage Centre.

3.5.2 Configuration Item Control and Updates (Enhanced Only)

Minor version, Patch and Security Hotfix

We will monitor OEM-published patch, security hotfix and version updates associated with configuration items, and review 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 the sourced RFC.

We will install an unlimited number of qualified and applicable software patches and OS minor version upgrades for configuration items. All patches or minor version upgrades are considered normal changes, therefore, all applicable change management processes apply.

If we determine an in-scope configuration item is susceptible to a new vulnerability, which is classified as low or medium, we will seek your 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.

As vendors vary their version / numbering releases, the following information serves as a guide and example of definitions of major, minor and maintenance hotfix, and their inclusion within the Enhanced Service variant.

- **Major feature version/release**: Each vendor version/release typically includes numbers (X.Y.Z). The “X” in the X.Y.Z nomenclature represents a major feature release, which usually includes a large number of new features and/or significant software architectural changes.
- **Minor feature version/release**: The “Y” in the X.Y.Z nomenclature represents a minor feature release, which usually includes a small to medium number of new features and typically minimal software architecture changes.
- **Maintenance/hotfix release**: The “Z” in the X.Y.Z nomenclature represents a maintenance release, which only includes bug fixes.

If we determine your configuration item is susceptible to a new low or medium vulnerability, we will seek your approval prior to taking any response steps. If a SOC engineer deems a new vulnerability as high in severity, we may take immediate response steps through an emergency RFC.

Major Version Upgrades

All major version upgrades are considered Project Orientated Requests (PORs) as they require careful planning, coordination, management, and roll-back options. Additionally, we consider all major version upgrades as high risk as it pertains to

your production environments. Subsequently we recommend that such works be underwritten and carried out by a member of our Consulting Services Team.

We will coordinate all major version upgrades with you 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.

Signature Updates

Where applicable, configuration item signature databases are automated and require connectivity between the configuration item and the Internet to download the updates. We will check that the signature updates are being updated successfully.

Signatures Failures

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

Signature Escalations

If the cause of the configuration item's inability to update signatures is an error or deficiency in the manufacturer's database, we will escalate the issue to the manufacturer on your behalf.

Your Responsibilities

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

Signature Implied Service Level Agreement

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

3.5.3 Configuration Item Backup (Enhanced Only)

We will maintain a backup of configuration items in case of failure, or where applicable, unless otherwise noted in the contract as your responsibility.

We will backup the whole configuration item system every 24 hours, which may be utilized for restoration in the case of a disaster recovery scenario. We retain 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.

We will take an additional configuration backup before an RFC is implemented and utilize the backup to roll back to the last known configuration in the event of a failure of the change or as requested by the Client.

We will back up 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 configuration item configuration

The scope of backup may differ between configuration items based on vendor files and configuration.

In a co-managed service, any change requested via a service request must include a request to back up a configuration item's configuration.

If the Security Device Management Services are co-managed and, during a configuration item failure a request is not made by your organization, we may at our discretion roll back to the previous available backup. We will not be responsible for any previous changes lost or loss of service as a result.

3.5.4 Configuration Item Restore and Out of Band (Enhanced Only)

The Remote Management Kit (RMK) provides Out of Band (OOB) management of configuration items. The RMK is deployed to premises where your infrastructure is located and integrated with the in-scope configuration items. It is not applicable or supported for virtual or cloud-based configuration items.

OOB management is utilized to perform remote troubleshooting and maintenance activities if any of your configuration items encounter a catastrophic failure or lose connectivity to your network.

The RMK is optional for applicable configuration items as part of the Security Device Management Enhanced service variant.

The RMK requirements and options are:

- Primary In-Band IP Address connectivity to your infrastructure via NTT's Security Appliance (NTTSA) through an auto-established VPN maintained by us.
- If the RMK is utilized, secondary OOB connectivity is mandatory and must be supplied by you. Connectivity options are outlined below:

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)

Connectivity Option
Dedicated ADSL to the Internet (per RMK)

Table 3 RMK Connectivity Options

The RMK is under complete control by us. You must not:

- direct any unauthorized traffic to the RMK
- attempt to login to the RMK
- tamper with the RMK
- attempt to perform any penetration test on the RMK without express written consent from us

Should both the primary and OOB solutions become inoperable or otherwise unavailable for our use, we reserve the right to suspend the Security Device Management Services for the applicable configuration items until the situation is remedied. We are not responsible for any incident involving a configuration item while connectivity to the RMK is unavailable.

Through the RMK, we provide restoration of backups to configuration items if a failure or roll back to a previous configuration is desired, provided that the Security Appliance has the relevant connectivity and is able to push a restore operation to the configuration item(s).

The RMKs are monitored and managed as part of the Service.

3.5.5 Configuration Item Status Reporting

Configuration item status reporting is available via Manage Centre. Status reports include version details and traffic light status.

3.6. Configuration Management

3.6.1 Service Request Fulfilment

Service request fulfilment focuses on requests for information, advice or access.

Service Request Management

Service requests are raised via Manage Centre. Attainment of various key performance metrics are tracked, monitored and reported by us on a monthly basis.

Request for Information

You may request information through Manage Centre about the performance, configuration or other aspects of configuration items. We will deduct the commensurate number of MACD service credits (if applicable) and provide the information in the service request.

Service Request Reporting

We record all incidents, service requests or changes in the ITSM system and reported back through Manage Centre.

Project Oriented Requests (PORs)

We will charge, and you agree to pay, the then-current applicable hourly rates for work associated with PORs including any change performed by you resulting in adverse effects that requires us to perform remediation work to restore the software / configuration item to return the 'in-scope' device proper working service.

3.6.2 Policy Management (Enhanced only)

We provide policy / rule set management of in-scope configuration items and SaaS applications via the use of MACD services. We evaluate, prepare, and implement policy / rule set changes via the change management process. See 3.6.4 Change Management (Enhanced Only).

Policy management enforces granular access and security policies that manage Internet usage by user, application, location, and device. Policy management is delivered via the third party management console.

3.6.3 Move, Add, Change, Delete (MACD) (Enhanced Only)

Technical service requests are administered through MACD service units and are requested via Manage Centre.

MACD service units are bundled within the Enhanced Service variant with the option to purchase additional MACD service units based on configuration item sizing (see *Table 4 MACD Service Units*). MACD service units are deducted in the execution of any client-sourced service requests pertaining to RFCs of configuration items. The number of MACD service units deducted per service request is based on a predefined list of standard tasks that we have derived by assessing the level of complexity to route accordingly to an appropriate SOC engineer.

The following table outlines the number of MACD service units bundled per device / SaaS application, annually with the Security Device Management Enhanced Service variant:

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

Table 4 MACD Service Units

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

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

You can view current MACD service unit usage on Manage Centre. MACD service unit usage is included within any scheduled Service reviews to ensure that you are operating in line with MACD availability. Should the MACD service unit balance

drop below a certain threshold, a notification will be sent to your contact for the purchase of additional MACD service units, if required.

Non-Standard Tasks Utilizing MACD Service Units

In the unlikely event that there is not a pre-existing classification for a service request, we consider this a non-standard task.

We will review non-standard tasks requested by you to determine:

- the apparent risk associated with performing the task.
- the likely impact of the change
- if we have the appropriate skills to action or implement the task
- if the non-standard task should become a standard task (based on demand / repeatability)

We will assess the non-standard task to determine the correct number of MACD service units. We will provide you with the number of MACD service units the task will incur for approval to proceed. Once approved by you, we will execute the service request for a non-standard pre-approved task. No service levels will apply to the execution of a non-standard task.

3.6.4 Change Management (Enhanced Only)

At your request, we will implement a RFC to configuration items in accordance with an associated MACD task or non-standard task.

Client –Sourced Requests

A valid client contact must submit a RFC case within Manage Centre.

NTT-sourced Requests

We may submit a RFC when a correct control change is necessary to resolve a problem or incident.

Change Reporting

All RFCs must be reported and tracked via Manage Centre including co-managed scenarios. The party making an RFC is required to open an applicable request with our Service Desk prior to implementation to ensure coordination between both parties.

Request for Change (RFC)

All types of RFCs follow our change management process and require our approval. We derive tasks per technology which correspond to the number of MACD service units utilized by each task. There are 3 (three) types of request for change outlined below:

Change Type	Description
Normal	Normal changes require approval (from NTT and the client respectively) before being implemented. Neither the client nor NTT is authorized to apply changes on behalf of the other without documented consent from appropriately authorized individuals (documented within a Change Approver Group on Manage Centre) from both parties via an RFC ticket resident in Manage Centre.
Standard	NTT is authorized by the client to apply changes without authorization from the client when a standard change ticket is raised via Manage Centre, however an NTT internal approval process is still valid.
Emergency	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 will work with the client during the change management process.

Table 5 Types of Change

Cancelling an RFC

You may cancel an RFC up to 2 (two) hours before any scheduled changes are committed to the configuration item configuration, in which case, any MACD service units that would have been deducted are cancelled.

If you need to reverse a change that has already been implemented, you must submit a new RFC via Manage Centre, in which case the commensurate MACD service units are deducted for both the original change and any subsequent reversal requested.

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 us to ensure a backup is taken
- for SaaS applications where the vendor does not support backup and rollback, ensure that all changes are documented so that the previous change can be identified and reverted back.
- 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 shared with you) to confirm whether the change was successful or not
- create a backup of the new configuration after the change is implemented
- for SaaS applications, you must perform user acceptance and functional tests within your production environment once changes are implemented
- update RFC ticket indicating whether the change was successful or not

It is imperative each change is documented via an RFC ticket in Manage Centre to ensure we can quickly troubleshoot if / when unanticipated negative consequences arise.

Exceptions

You understand that any exceptions that may arise due to deviation from or circumventing the processes described herein may result in an unstable and/or unsecured configuration items and/or non-compliant configurations. Accordingly, you release NTT from any liability resulting in outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to any change made by you.

You agree that any work performed by NTT to troubleshoot issues that are directly attributable to a change made by you is billable at the current NTT engineer's hourly rate.

Client Responsibilities

You agree only appropriately trained and skilled engineers will perform changes in a co-managed environment. Also, you understand that we reserve the right to bill for incremental troubleshooting work that we perform as a result of:

- you not accurately recording changes on your in-scope configuration item(s)
- you not notifying us about the changes being made with at least 1 (one) full business days' notice
- you performing work that violates OEM support agreements or leads to in-scope configuration items negatively affecting your production environment

NTT's Responsibilities

We will review incidents, service requests and documentation regarding changes performed by you and may seek clarification.

Change Impact Analysis

Our change impact analysis process applies to all RFCs (pre- and/or post-implementation). We will conduct a change impact analysis prior to implementation of any RFC, including patch and version management or PORs to ensure:

- hardware/software meets all prerequisites
- backups of previous version/configuration exists
- any change does not compromise your network, service or that of NTT
- any change is relevant to your environment
- any change can be implemented within the requested time frame

We consider the change impact analysis complete and the implementation period will begin when your organization has addressed all issues raised during the analysis (if applicable), and the engineer acknowledges receipt of a valid RFC.

We review the incident cases, service request cases, and documentation regarding RFC cases in the event of a co-managed service and may seek clarification.

4. Service Options

4.1.1 Co-Management (Option for Enhanced Only)

Co-management is a chargeable option, which must be purchased to be enabled. In a co-managed scenario, the following conditions apply:

- configuration item availability (service level agreement) is not applicable.
- configuration item configuration and policy changes can only be made by specific contacts raising a service request via Manage Centre
- access to devices and the management console for SaaS applications must be restricted to named user accounts and/or defined from specific client internal locations/workstations where applicable (for example, IP addresses/subnets)

For NTT to provide effective support, you must:

- notify us 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 RFC within Manage Centre
- explicitly request a backup via a request made via Manage Centre
- if applicable, and upon completion, provide a report/status update from your internal change management process to ensure we are aware of all the changes occurring to configuration items
- make changes to configuration items such that there is a clear audit trail indicating the party responsible for the change, the date of the change and your change control identification
- make each change 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 our service administration rules must be agreed by the SOC prior to their implementation.

You accept that 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 configurations. Consequently, you will release NTT from any liability resulting from outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to the changes implemented directly by you. We may, at our 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. Service Management

Our desire is to maximize the value you receive from Managed Security Services through effective engagement, communication and information sharing. Our focus is to enhance your service experience and provide your organization with insight to enable your business decisions.

5.1. Service Desk

Our regional Managed Service Centre (MSC) is your primary Service interface, available to you 24/7/365. The NTT MSC coordinates incidents, and service requests, as well as system administration functions.

The service desk logs, tracks, and closes all tickets (incidents and service requests) in the NTT service management system. Tickets can be logged through the following methods:

- event driven (through monitoring of the environment)
- directly reported to us by you through the service desk
- directly reported to us by you via the NTT Manage Centre portal
- directly reported by Security Operations Centres (SOCs) via our integrated service desk.

5.2. Service Level Management

As a Client of NTT's Managed Security Services you will be assigned a Service Delivery Manager.

Depending on the complexity and/or size of your environment, and the mix of products and services, we may recommend contracting a Technical Account Manager (TAM) function as described *5.2.2. MSS Technical Account Manager (Optional)*.

5.2.1 NTT Service Delivery Manager (SDM)

Service delivery management provides governance and control across the various service features, processes, and systems necessary to manage the full lifecycle of the Service.

We will assign a Service Delivery Manager (SDM) to be responsible for service level management, and to act as an advocate for your organization within NTT. The SDM is the primary interface who will manage the service delivery relationship between your organization and NTT. The SDM is responsible for scheduling and running all service management review meetings, and ensuring all processes and documentation are in place to manage your Services.

Deliverables of the SDM include:

- establish client relationship
- capture and manage minutes, agenda items, actions, and decisions
- change management issue management
- escalation management

- risk management
- service level monitoring, reporting and management
- service review meeting

5.2.2 MSS Technical Account Manager (Optional)

The MSS Technical Account Manager option is a security management function that provides technical and risk-based oversight and advocacy services for you. The Service is delivered through the MSS Technical Account Manager Team who assign and designate Technical Account Managers to clients who subscribe to the Service providing the full depth and breadth of our cybersecurity capabilities.

The MSS Technical Account Manager Team leverages security best practices and an expansive knowledge base to deliver globally consistent security programs tailored to your specific needs and regulatory requirements. They are committed to developing long-term relationships with you to gain a deep understanding of your business objectives. This includes understanding your strategic initiatives, risk profile by industry or sector and cybersecurity maturity level assessments. This knowledge and level of technical engagement ensures you benefit from an optimized service aligned with your organization's business imperatives.

The MSS Technical Account Manager Team are an additional component of our MSS delivery model, and provide cybersecurity insights beyond MSS. Coupled with our 24/7 SOC teams, the MSS Technical Account Manager Team provides operational support and consultative guidance in alignment with your business priorities and technology roadmaps.

The MSS Technical Account Manager Team provides increased Client intimacy by being available on-site (if geo permits) as needed to provide technical guidance and to operate as an extension of your security team. You can benefit from MSS Technical Account Manager Team support of internal and external stakeholder management while they face challenges implementing security controls across your enterprises.

The MSS Technical Account Manager Team are the client advocates who identify and track action items and service requests that have been raised via the Service Desk to reduce the time to respond to your requests. The MSS Technical Account Manager Team also provides a quality control function to ensure delivery excellence, maintain high levels of client satisfaction, achieve project success, and drive continual service improvement.

The SOC provides 24/7 support and although the MSS Technical Account Manager Team are not a 24/7 resource, the MSS Technical Account Manager Team is included in the escalation path for security incidents whereby intimate knowledge and proximity to you provides further context to aid in assessment and response activities. Overall, the team share observations and makes recommendations to improve your cybersecurity maturity and help you to manage risk.

6. Service Transition

Our approach to transition aims to ensure that both organizations enter the transition with a clear idea and understanding of the goals and objectives of the transition.

6.1. Objectives of Service Transition

- To ensure the absolute minimal business disruption during the transition of the managed service
- To facilitate a smooth and trouble-free transition
- To determine and manage realistic transition timeframes
- To establish an operational baseline for the global managed services delivery organization that will be responsible for delivering the service post-transition
- To facilitate and conclude the contracting process
- To develop and build a sound business relationship from the onset
- To align your expectations with service delivery capabilities and constraints
- To ensure our people understand your business from the onset to deliver reliable, stable and excellent service

6.2. Transition Methodology

We use a formal transition methodology, developed in-house from industry-leading best practices and years of practical experience.

Our Service Transition Manager is responsible for managing the transition process with you and your organization. As part of the service activation process, the required tools and systems are set up and activated for the managed service to go live.

The typical duration for Service Transition is 12 elapsed weeks, although timing will depend on the size and complexity of the environment.

6.3. Dependencies

6.3.1 Software/Appliances License

You are 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 service contract period. You must ensure that licenses are valid at the start of the Service contract through to the end of the Service contract.

6.3.2 Manufacturer Hardware/Software Support

Managed configuration items must have full manufacturer support at all times during the service contract period. The manufacturer support contract must have partner enablement, where applicable. In order to raise support tickets with the manufacturer on your behalf, NTT must be added as an authorised vendor support contact and/or partner. We will not provide any services for any configuration item

not covered by a valid maintenance contract. Neither will we 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 contract or subsequent 12-month renewal period. The Service does not include the replacement of obsolete hardware/software.

6.3.3 Software Updates (Subscriptions)

You are responsible for all manufacturer's software subscriptions (for example, software updates) for any configuration items to be managed. Such subscriptions are required for the duration of the Service contract period. You must ensure that any software subscriptions are valid at the start of the Service contract through to the end of the Service contract. We will will not provide any services for expired subscriptions.

6.3.4 Limitations of Use

Only the manufacturers' security application/operating system software, relevant and/or necessary software/applications and software provided by NTT (where applicable) to support our Service must be run on the configuration item.

6.3.5 Secure System Management

We highly recommend that any in-scope configuration items have a secure configuration/policy implemented prior to the start of any Service contract (including renewals). This must be maintained for the full Service period.

6.3.6 Secure Facility

It is your responsibility to provide and maintain a physically secured and environmentally-suitable facility for any manufacturer hardware/software and associated NTT-supplied hardware/software, including appropriate rack space and power.

6.3.7 Virtual Environment

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

6.3.8 Managed Devices

Managed devices must be healthy, functional and tuned before we will accept the management responsibility during the deployment phase, where:

- **'Healthy'** means there are no known hardware/software issues, or bugs affecting the operation or management of the configuration item.
- **'Functional'** means the configuration item has been specified and designed correctly, configured and operationally effective.

- **'Tuned'** means the configuration item has been configured according to the needs and relevance of your environment, including minimizing false positive alerts and ensuring redundant or unnecessary configurations are removed.

Appendix A Service Level Agreements

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Request Response	NTT will assign a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1&P2	60 Mins	5% of Monthly Service Fee	N/A	N/A
		P3&P4	4 Hours			
Request Complete	NTT will resolve a Service Request with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1	2 Business days	95% Service Units of the Request	95% Service Units of the Request	N/A
		P2&P3	5 Business days			
		P4	10 Business days			
Incident Management – Response	NTT will assign a Incident ticket with priority ____ within ____ minutes of receiving the ticket at NTT`s Service Desk.	P1&P2	30 Min	N/A	N/A	24/7
		P3&P4	60 Min			
Incident Management – Restore – Enhanced Only	NTT will restore the Service associated with a priority ____ incident within ____ hours of receiving the ticket at NTTS Device Management Team.	P1	4 hrs	5% of Monthly Service Fee	Max up to 25% of Monthly Service Fee	24/7
		P2	8 hrs			
		P3&P4	24 hrs			
Incident Management – Resolve – Enhanced Only	NTT will resolve a priority ____ incident within ____ hours of receiving the ticket at NTTS Device Management Team.	P1	8 Hours	N/A	N/A	24/7
		P2	16 Hours			
		P3&P4	48 Hours			
Emergency Change Response – Enhanced Only	NTT will assign an Emergency Change ticket within ____ minutes of receiving the ticket at NTT's Service Desk	N/A	30 Min	N/A	N/A	N/A
Change Response – Enhanced Only	NTT will assign an Change ticket within ____ minutes of receiving the ticket at NTT's Service Desk	N/A	60 Min	N/A	N/A	N/A
Change Implementation – Complete – Enhanced Only	NTT will complete changes before the end of the change window as mutually agreed upon between client and NTT.	N/A	95%	N/A	N/A	

Category	Description	Priority	SLA	Service Credits	Service Credit Limit	Service Calendar
Restore Notification (Service Level Objective) – Notify – Enhanced Only	NTT will provide a restore notification for every Incident ticket within ____ minutes of restoring the service.	N/A	30 Min	N/A	N/A	
Resolve Notification (Service Level Objective) – Notify – Enhanced Only	NTT will provide a resolve notification for every Incident ticket within ____ minutes of restoring the service.	N/A	30 Min	N/A	N/A	

Table 6 – Service Level Agreements

Appendix B