Client Service Description

Security Device Management

01 October 2019 | Document Version 1.5
Client Service Description

{Subject}

NTT contact details
We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:
Bob Gordon – Services Product Portfolio Director – Security, Phone: +1 203 446 4942
NTT Limited
✉️ bob.gordon@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shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.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
This document is valid until 11 July 2019 and, in the absence of any other written agreement between the parties, 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.
Client Service Description

{Subject}

Document Preparation

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepared:</td>
<td>Paul Asdagi</td>
<td>12 Sep 2018</td>
</tr>
<tr>
<td>Prepared</td>
<td>Mike Oberholtzer</td>
<td>01 Feb 2019</td>
</tr>
<tr>
<td>Prepared</td>
<td>Bob Gordon</td>
<td>06 Jun 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Sharon Witheriff</td>
<td>07 Jun 2019</td>
</tr>
<tr>
<td>Updated</td>
<td>Bob Gordon</td>
<td>01 Oct 2019</td>
</tr>
</tbody>
</table>

Release

<table>
<thead>
<tr>
<th>Version</th>
<th>Date Released</th>
<th>Pages</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>06 Jun 2019</td>
<td>Internal DRAFT</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>07 Jul 2019</td>
<td>Internal DRAFT</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>01 Oct 2019</td>
<td>Rebrand</td>
<td></td>
</tr>
</tbody>
</table>

© 2020 NTT Pty Limited. The material contained in this document, including all attachments, is the copyright of NTT Pty Limited. No part may be reproduced, used or distributed for any purpose, without the prior written consent of NTT Pty Limited. This document, including all attachments, is confidential and use, reproduction or distribution of this document or any part of it for any purpose, other than for the purpose for which it is issued, is strictly prohibited. Uptime® is a registered trademark of NTT.

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

1. Service Description ................................................................. 6  
   1.1. Overview ............................................................................. 6  
   1.2. Service Matrix ................................................................. 7  
   1.3. Supported Device List ...................................................... 8  
   1.4. NTT’s Managed Security Services Portfolio ..................... 9  

2. Detailed Service Description ..................................................... 10  
   2.1. 24/7 Security Operations Center Coverage ...................... 10  
   2.2. Operation Hours ............................................................... 11  
   2.3. Language Support ............................................................. 11  
   2.4. Device Management ......................................................... 11  
   2.5. ITSM Service Management .............................................. 12  
   2.6. Monitoring ......................................................................... 12  
   2.7. Engineering ....................................................................... 13  
   2.8. Escalation Management .................................................... 13  

3. Detailed Service Features .......................................................... 15  
   3.1. Health and Availability Monitoring .................................. 15  
   3.2. Incident Management ....................................................... 15  
   3.3. Asset Tracking and Reporting ......................................... 16  
   3.4. Service Request Fulfilment .............................................. 20  
   3.5. Problem Management ..................................................... 24  

4. Our Approach to Service Operations .................................... 26  
   4.1. Service Experience ......................................................... 26  
   4.2. Service Desk ................................................................. 26  

5. Service Transition ................................................................. 29  
   5.1. Objectives of Service Transition .................................... 29  
   5.2. Transition Methodology .................................................. 29  
   5.3. Dependencies ................................................................. 29  

6. Service Management .............................................................. 31
6.1. Service Level Management ........................................................................... 31

Appendix A Service Level Agreements ......................................................... 32

List of Figures
Figure 1 – Global Managed Security Service Platform ........................................ 9
Figure 2 – Global Delivery Model .................................................................. 10
Figure 3 – Continual Improvement Process ...................................................... 11

List of Tables
Table 1 – Service Matrix ............................................................................. 8
Table 2 – Supported Device Vendor Table ................................................... 8
Table 3 – MACD Service Units .................................................................. 21
Table 4 – Types of Change .......................................................................... 23
Table 5 – Service Level Agreements ............................................................... 33
1. Service Description

1.1. Overview

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

Managing security devices, however, requires a specific and specialized skill set that demands constant attention, training and upkeep. Keeping security devices updated and patched while monitoring them 24/7 is a challenge for all organizations, big and small.

We reduce that burden with our Security Device Management Service that follows industry best practices to provide appropriate service fulfilment and change management processes, and request, incident, and change management processes that help you keep your security devices available while maintaining compliance with applicable regulatory requirements.

NTT’s Security Device Management – Standard Service utilizes the Global Managed Security Services Platform (GMSSP) to provide 24/7 health and availability monitoring of devices and notifies you of any incidents which may cause disruption to your business. In this service offering you maintain complete control of your security infrastructure but leverage NTT’s 24/7 Security Operation Centers (SOC) capabilities.

NTT’s Security Device Management – Enhanced Service builds on the standard Service Package to offer a 24/7 fully managed service including health and availability, 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.

NTT’s Security Device Management Services provide:

- on-demand device configuration and tuning
- timely updates and patch management
- continuous device health and availability monitoring
- 24/7 coverage via 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 securely 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
- superior service experience

1.2. Service Matrix

The Security Device Management Services are available in two distinct Service Packages, which consist of a core set of elements, such as service transition and associated service elements such as incident management.

<table>
<thead>
<tr>
<th>Service Feature and Element</th>
<th>Service Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Health and Availability Monitoring</strong></td>
<td></td>
</tr>
<tr>
<td>Health and availability monitoring</td>
<td>✔️</td>
</tr>
<tr>
<td>Health and availability improvement and recommendation</td>
<td>✔️</td>
</tr>
<tr>
<td>Health and availability change implementation</td>
<td></td>
</tr>
<tr>
<td><strong>Incident Management</strong></td>
<td></td>
</tr>
<tr>
<td>Incident generation</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident diagnosis</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident resolution</td>
<td>✔️</td>
</tr>
<tr>
<td>Incident reporting</td>
<td>✔️</td>
</tr>
<tr>
<td><strong>Asset Tracking and Reporting</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration item recording</td>
<td>✔️</td>
</tr>
<tr>
<td>Configuration item control and updates</td>
<td>✔️</td>
</tr>
<tr>
<td>Configuration item backup</td>
<td>✔️</td>
</tr>
<tr>
<td>Configuration item restore + OOB</td>
<td>✔️</td>
</tr>
<tr>
<td>Configuration item status reporting</td>
<td>✔️</td>
</tr>
<tr>
<td>[Option] Co-Management</td>
<td></td>
</tr>
<tr>
<td><strong>Capacity Management</strong></td>
<td></td>
</tr>
</tbody>
</table>
Service Feature and Element | Service Packages
--- | ---
Capacity monitoring and reporting | ✓
Capacity improvement recommendation | ✓
Capacity Planning | ✓
Capacity Change Implementation | ✓

### Service Request Fulfilment

<table>
<thead>
<tr>
<th>Service Package</th>
<th>Service Packages</th>
</tr>
</thead>
</table>
| Service request management | ✓
| Move, Add, Change, Delete (MACD) fulfilment | ✓
| Change management | ✓

### Problem Management

<table>
<thead>
<tr>
<th>Feature</th>
<th>Service Packages</th>
</tr>
</thead>
</table>
| Problem Identification and Recording | ✓
| Problem Reporting | ✓
| Solution Identification and Recording | ✓
| Solution Implementation | ✓

### Service Transition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Service Packages</th>
</tr>
</thead>
</table>
| Transition | ✓

#### Table 1 – Service Matrix

#### 1.3. Supported Device List

Supported vendors for the Security Device Management services are:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Cisco</th>
<th>F5 Networks</th>
<th>FireEye</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkpoint</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fortinet</td>
<td>Imperva</td>
<td>Juniper</td>
<td>McAfee</td>
</tr>
<tr>
<td>Palo Alto</td>
<td>Pulse Secure</td>
<td>Symantec</td>
<td></td>
</tr>
</tbody>
</table>

#### Table 2 – Supported Device Vendor Table

Note. Device support varies between the Standard and Enhanced Service Packages. Please contact your NTT Sales Executive for a more detailed list of devices and which packages they are supported under.
1.4. **NTT’s Managed Security Services Portfolio**

Our portfolio of Managed Security Services helps reduce the burden of constant and proactive network monitoring, advanced security analysis, and global intelligence correlation. All our Managed Security Service offerings are powered by the Global Managed Security Service Platform (GMSSP) combined with our proven combination of people, process and technology.

![Global Managed Security Service Platform](image)

*Figure 1 – Global Managed Security Service Platform*

The portfolio of Managed Security Services consists of:

- **Threat Detection Services.** The Threat Detection Services include Standard and Enhanced Service Packages for advanced detection, investigation and reporting of Security Incidents.

- **Monitoring Services.** The Enterprise Security Monitoring Services include Standard and Enhanced Service Packages for security detection and compliance reporting.

- **Security Device Management Services.** The Security Device Management Services include Standard and Enhanced Service Packages for management of a broad range of security technologies.

- **Vulnerability Management.** The Vulnerability Management Services deliver customized vulnerability scanning, with a variety of compliance and reporting options.
2. **Detailed Service Description**

2.1. **24/7 Security Operations Center Coverage**

Security Device Management Services are delivered by multiple Security Operations Centers (SOC) across the globe, manned on a 24/7 basis by Security Analysts with extensive vulnerability and threat detection knowledge and supported by strong technical capabilities of the Global Managed Security Service Platform (GMSSP).

Security Analysts will assist with scan maintenance, troubleshooting, configuration, launching on-demand scans as well as stopping scans, asset maintenance and general service and or reporting questions.

![Globally integrated service delivery model](image)

*Figure 2 – Global Delivery Model*

We provide operational excellence through a network of SOCs strategically located around the globe with ISO27001 certification ensuring a consistent and reliable security program. Additionally, SOC2 compliance is held by US and Nordic-based SOCs.

We will deliver the Security Device Management Services through our SOCs and you are provided with the contact details of relevant SOCs through the service transition process. We may deliver the Security Device Management Services from any of our SOCs at any given time, as deemed necessary. Your data may subsequently be held and processed in any of the SOC locations, unless supported by a prior application for non-standard services and a written agreement and confirmation of approval.

We follow Information Technology Infrastructure Library (ITIL) for repeatable and consistent service delivery, and specifically for the Security Device Management
Services, for service operation. The purpose of service operation is to co-ordinate and carry out activities and processes required to deliver and manage the Security Device Management Services. Key operational processes link together to provide an effective overall support structure with distinct processes aligned to our SOCs and service tools.

![Continual Improvement Process Diagram]

**Figure 3 – Continual Improvement Process**

All NTT services are included in our company-wide Continual Service Improvement process.

### 2.2. Operation Hours

The Security Device Management Services are delivered through the SOCs, and the regional Managed Services Centers (MSCs) which both operate 24/7.

### 2.3. Language Support

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

### 2.4. Device Management

The responsibilities for managing devices is dependent on the type of management service selected by you. The types of management services are detailed in the following three sections.
2.4.1 Standard Management

You provide NTT with privileged access to configuration item(s).

We will create one administrator account for you and will securely store the credentials and password. If, during an emergency where we are unable to make a change or access the configuration item/management infrastructure, the primary security contact will be provided with the credentials and password.

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

Barring co-managed devices, you agree not to create any administrator or other change-capable accounts (i.e. ‘super user’) on configuration items. If required, you must request creation of such administrator accounts via a service request. We perform periodic and ongoing auditing of all administrator accounts.

2.4.2 Co-Management

NTT and you and/or your nominated third party and/or an NTT Group Operating Company have access to configuration item(s) with the ability to make updates and configuration changes. In a co-managed scenario, specific conditions apply.

2.4.3 Read Only Access

You can be provided with read-only access to configuration item(s).

2.5. ITSM Service Management

NTT’s ITSM system manages all incidents, service requests, request for changes, and problems following ITIL wherever appropriate. Access is provided to appropriate staff only.

2.6. Monitoring

NTT's ITSM system manages all incidents, service requests, request for changes, and problems following ITIL wherever appropriate. Access is provided to appropriate staff only.

2.6.1 Protocols

Your configuration items are monitored utilising multiple protocols including ICMP and SNMP v3.

2.6.2 Event Feed

The correlated event feed from the on-premises collector is sent over a VPN to the monitoring server in the GMSSP infrastructure.
2.7. **Engineering**

2.7.1 **Configuration Item Access**

Command line access is secured over SSH v2. SSH access is provided from a trusted 'jump host' within the GMSSP infrastructure.

2.7.2 **Application Access**

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

2.7.3 **Backup (Enhanced Only)**

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

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.

2.8. **Escalation Management**

We utilize escalation processes and defined responsibilities for addressing escalated matters. To escalate a configuration item incident, request for change or service request, you may telephone or email the service desk (quoting the reference number). An NTT Escalation Manager is then assigned within a 24/7 service calendar 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 you, NTT and relevant third parties
- regularly communicating escalation status to:
  - you
  - the security Client Services Manager (if assigned)
  - the NTT Account Executive
  - any other parties relevant to the escalation
- regularly updating and seeking the advice and support of NTT management
For the duration of an escalation, ensuring all appropriate personnel are available to support the agreed action plan.

We may downgrade an escalated security incident, incident, change request or service request if it is being managed to a scheduled time frame, or resolution has been provided to you and is in the process of being tested. If you initiated the escalation, we will obtain your approval prior to downgrading an escalated security incident, incident, change request or service request.

You may request that your incident, service request or problem be escalated to a higher priority at any time provided that sufficient justification is provided. Upon review, the SOC Manager is responsible for agreeing any urgent change.
3. **Detailed Service Features**

3.1. **Health and Availability Monitoring**

3.1.1 **Health and Availability Monitoring**

The NTT Device Management Services monitors key performance indicators of configuration item's service state and resource utilization to determine health, performance and availability. The Services automatically generate 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 5.3. You will be notified and kept up to date of issues with health and availability via the incident ticket available on the Security portal.

3.1.2 **Health and Availability Improvements and Recommendation**

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 applicable service levels and where we do not have access to make changes, if we make recommendations to you which have not been implemented and in-scope configuration item(s) 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.

3.1.3 **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. **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 NTT Service Delivery teams on a 24/7/365 basis. We manage incidents according to their assigned priority as outlined in Error! Reference source not found.. Error! Reference source not und.
3.2.1 Incident Generation

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

For incident tickets raised via the Managed Centre portal, 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 relevant priority assigned.

3.2.2 Incident Diagnosis

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

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 the portal.

3.2.3 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 and the incident will be moved to a ‘closed’ state
- you confirm incident is not resolved, the ticket will be moved back to a ‘working’
- you do not respond, and the incident will be auto closed after 10 days

3.2.4 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 the portal.

3.3 Asset Tracking and Reporting

3.3.1 Configuration Item Recording

We will record and track your configuration items with information available within the Security portal.
3.3.2 Configuration Item Control and Updates (Enhanced Only)

**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 Request for Change (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 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 client production environments. Subsequently we recommend that such works be underwritten and carried out by a member of the consulting services team.

We will coordinate all major version upgrades with you and may agree to utilize the SOC and Move, Add, Change, Addition (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.

**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.

**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.

Implied Service Level Agreement

If a 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 vendors’ third-party supplier agreement.

3.3.3 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 back up the whole configuration item system every 24 hours which may be utilized for restoration in the case of a disaster recovery scenario. We will retain a maximum of 7 (seven) previous full system configuration item backups onsite via the Security Appliance. This is subject to storage availability on the Security Appliance. By default, no system backups are stored offsite. An option to store offsite backups is available on request.

If the off-site backup option is selected, we will store 1 (one) off-site system backup and 1 (one) configuration backup. When 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.

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.

### 3.3.4 Configuration Item Restore and OOB (Enhanced Only)

The Remote Management Kit (RMK) provides Out-of-Band (OOB) management of 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 owned by and under complete control by us. You must not:

- direct any unauthorized traffic to the RMK device
- 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 item(s) 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 as part of the Service.

### 3.3.5 Configuration Item Status Reporting

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

### 3.3.6 Co-Management (Option for Enhanced Only)

In a co-managed scenario, the following conditions apply:

- Co-management is only available as an option within the Enhanced Service Package.
- Configuration item availability (service level agreement) is not applicable.
- Configuration Item configuration and policy changes can only be made by raising a service request via the Managed Centre portal.
3.4. Service Request Fulfilment

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

3.4.1 Service Request Management

Service requests are raised via the Managed Centre Portal. Attainment of various key performance metrics are tracked, monitored and reported within NTT on a monthly basis.

Request for Information

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

Service Request Reporting

All incidents, service requests, problems or changes are recorded in the ITSM system and reported back through the Managed Centre portal.

Project Oriented Requests

We will charge, and you agree to pay, the then-current applicable hourly rates for work associated with PORs. If any change performed by you results in adverse effects and requires remediation work be performed by us to restore the
software/configuration item to proper working service, you agree to pay us the then-current Engineering hourly rate to return the ‘in-scope’ device to normal operating run-state.

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

Technical service requests are administered through a Move, Add, Change, Delete (MACD) service unit model and are requested via the Manage Centre portal as described in section Error! Reference source not found..

MACD service units are bundled within the Enhanced Service Package with the option to purchase additional MACD service units, and are based on configuration item sizing (see Table 3 – 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 with the Security Device Management Enhanced Service Package:

<table>
<thead>
<tr>
<th>Size</th>
<th>MACD Service Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>25</td>
</tr>
<tr>
<td>Medium</td>
<td>30</td>
</tr>
<tr>
<td>Large</td>
<td>40</td>
</tr>
<tr>
<td>large</td>
<td>50</td>
</tr>
</tbody>
</table>

*Table 3 – MACD Service Units*

Note. 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, 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 the Security portal. 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 if:
● we have the appropriate skills to action or implement the task
● 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 pre-approved task.

3.4.3 Change Management (Enhanced Only)
At your request, we will implement an RFC to configuration items in accordance with an associated MACD task or non-standard task as outlined in section Error! Reference source not found.

NTT-sourced Requests
We may submit an RFC when a correct control change is necessary to resolve a problem or incident.

Change Reporting
All RFCs must be reported and tracked via the portal including co-managed scenarios.

The party making an RFC is required to open an applicable request with our service desk.

Request for Change (RFC)
All types of RFCs follow our change management process and require our approval. We 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:

<table>
<thead>
<tr>
<th>Change Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Normal Changes require approval (from NTT Security and client respectively) before being implemented. Neither client nor NTT Security 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 Security portal) from both parties via an RFC case resident in the NTT Security portal.</td>
</tr>
<tr>
<td>Standard</td>
<td>NTT Security is authorized by the client to apply changes without authorization from the client when a standard change ticket is raised via the NTT Security portal, however an NTT Security internal approval process is still valid.</td>
</tr>
<tr>
<td>Emergency</td>
<td>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 Security will work with the client during the change management process.</td>
</tr>
</tbody>
</table>
Table 4 – Types of Change

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

If you would like to reverse a change that has already been implemented, you must submit a new RFC via the Security portal, in which case the commensurate MACD service credits 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.
- 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.
- Update RFC ticket indicating whether the change was successful or not.

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

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

Change Impact Analysis
NTT’s Change Impact Analysis process applies to all RFCs (pre- and/or post-implementation). We review incidents, service requests and documentation regarding RFCs in the event of a co-managed service and may seek clarification.

We will conduct a Change Impact Analysis prior to implementation of any RFC, including RFC, 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.

3.5. **Problem Management**

3.5.1 **Problem Identification and Recording**

NTT Security follows 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 Security ITSM tool and the NTT Security 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 client’s environments
• compound problems caused by multiple incidents of different natures within a single client environment
• notification of the problem from the manufacturer
• lack of timely patch from the manufacturer to address security vulnerability/s
• trend analysis

3.5.2 **Problem Reporting**

All problems are recorded in the ITSM system and reported through the NTT Security portal.

3.5.3 **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.

3.5.4 **Solution Implementation (Enhanced Only)**

You and NTT Security 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.
4. **Our Approach to Service Operations**

4.1. **Service Experience**

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.

4.2. **Service Desk**

NTT’s regional Managed Service Centre (MSC) is your primary Service interface, available to you 24/7/365. The MSC coordinates incidents, and service requests, as well as system administration functions. They interact with you from a Service contract perspective, and as such, will have access to contract details, service information (service entitlements), site data and contact information, site and network diagrams, and configuration item/IT service data. They also ensure the knowledge management system is updated and kept current for your network infrastructure, action any service requests.

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 Manage Centre portal

When contacted by you, the MSC will manage your request through to resolution, including:

- initial classification and prioritization
- assignment to correct resolver group
- ticket updates
- closure once resolved/completed or as contracted

4.2.1 **Manage Centre Portal**

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

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

Figure 6: Manage Centre Portal

4.2.2 Online Dashboards and Charts

Reporting is provided via NTT’s Manage Centre portal, through a mixture of interactive dashboards, charts and downloadable reports. Through Manage Centre, users 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

1 The Managed Centre Portal provides a consolidated view of all your NTT managed services some functionality such availability, capacity and performance data do not apply to security services.
Interactive reporting is available for:

- service levels
- task-related data e.g. incidents, requests, changes
5. **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.

### 5.1. 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.

### 5.2. Transition Methodology

We use a formal transition methodology, developed in-house from industry-leading best practices and years of practical experience with the transition of operations from its clients and/or incumbent service providers. It is a formal methodology that allows flexibility for adjustment to cater for a wide spectrum of operational services, assets, staff, policies, process, standards and architectures to be transferred to us.

NTT’s Service Transition Manager is responsible for managing the transition process with you and your organization and coordinating with our Centre of Excellence (COE) Transition team. The COE Transition team is responsible for running the service activation process to enable service operations. As part of the service activation process, the tools and systems are setup and activated for the managed service to go live.

The typical duration for service transition is 12 weeks, although timing will depend on the size and complexity of your environment.

### 5.3. Dependencies

#### 5.3.1 Managed Devices

Managed devices must be Healthy, Functional and Tuned before we will accept the management responsibility during the deployment phase.
‘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.
6. Service Management

6.1. Service Level Management

Depending on the complexity and/or size of your environment and the mix of products and services, we may recommend additional Service Delivery Management options.

6.1.1 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 Security Device Management services.

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 NTT SDM is the primary interface who will manage the Service Delivery relationship between your organization and NTT. The SDM is responsible for scheduling, running all service management review meetings, and ensures 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
- work with Service Transition teams

6.1.2 Technical Account Manager (TAM) (Option)

The Technical Account Manager (TAM) is an optional resource that provides overall account management and specialized technical support to you by responding to action items, emails, and customer calls, and by proactively initiating actions to ensure client satisfaction. The TAM is the point of contact for incidents and service requests that are outside the scope of support provided by the SOC. The TAM also manages designated accounts both by responding to technical questions, issues, and opportunities; as well as by overall management of requests and general account satisfaction levels. This position is primarily technical in nature, with a high level of customer interface, and requires strong prioritization and project skills.
## Appendix A  Service Level Agreements

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Priority</th>
<th>SLA</th>
<th>Service Credits</th>
<th>Service Credit Limit</th>
<th>Service Calendar</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability - Client Portal</strong></td>
<td>The NTTS Portal is available 24 hours a day, 365 days a year with a 99.8% up-time guarantee (not including scheduled maintenance windows).</td>
<td>N/A</td>
<td>99.5%</td>
<td>5% of Monthly Service Fee</td>
<td>25% of Monthly Service Fee</td>
<td>24x7</td>
</tr>
<tr>
<td><strong>Emergency Request assignment response</strong></td>
<td>NTT will assign a Service Request ticket within 30 minutes from the client assigning the Service Request ticket to the NTT Service Desk.</td>
<td>N/A</td>
<td>30 mins</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Standard change / Normal Request assignment response</strong></td>
<td>NTT will assign a Service Request ticket within 30 minutes from the Client assigning the Service Request ticket to the NTT Service Desk.</td>
<td>N/A</td>
<td>60 mins</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Request Complete - Emergency request (RFC)</strong></td>
<td>P1</td>
<td>2 Business days</td>
<td>100% Service Units of the Request</td>
<td>100% Service Units of the Request</td>
<td>24/7</td>
<td></td>
</tr>
<tr>
<td><strong>Request Complete - Request for information/Standard change</strong></td>
<td>P1</td>
<td>2 Business days</td>
<td>100% Service Units of the Request</td>
<td>100% Service Units of the Request</td>
<td>24/7</td>
<td></td>
</tr>
<tr>
<td><strong>Device Availability - Standalone devices</strong></td>
<td>A device in a standalone configuration managed by NTT will be available 24 hours a day, every day of the year with a 99.8% uptime guarantee excluding scheduled maintenance windows (calculated monthly).</td>
<td>N/A</td>
<td>99.8%</td>
<td>5% of Monthly Service Fee</td>
<td>Max up to 25% of Monthly Service Fee</td>
<td>24/7</td>
</tr>
<tr>
<td><strong>Device availability – High availability pair</strong></td>
<td>Devices in an HA Pair configuration managed by will be available 24 hours a day, every day of the year with a 99.9% uptime guarantee excluding scheduled maintenance windows (calculated monthly).</td>
<td>N/A</td>
<td>99.9%</td>
<td>5% of Monthly Service Fee</td>
<td>Max up to 25% of Monthly Service Fee</td>
<td>24/7</td>
</tr>
</tbody>
</table>
# Client Service Description

{(Subject)}

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Priority</th>
<th>SLA</th>
<th>Service Credits</th>
<th>Service Credit Limit</th>
<th>Service Calendar</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incident Management response</strong></td>
<td>NTT will assign a Priority (P*) Incident ticket within (R*) time from Client assigning the Incident ticket to the Service Desk. P*=P1-P4, R*=Response</td>
<td>P1</td>
<td>30 mins</td>
<td>N/A</td>
<td>N/A</td>
<td>24/7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P2</td>
<td>60 mins</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>P3, P4</td>
<td>2 hrs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Incident Management restore</strong></td>
<td>NTT will restore service associated with a Priority (P*) incident within (R*) hour(s) of Incident ticket assignment to the NTTS Device Management Team. P*=P1-P4, R=Response</td>
<td>P1</td>
<td>4 hours</td>
<td>5% of Monthly Service Fee</td>
<td>Max up to 25% of Monthly Service Fee</td>
<td>24x7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P2</td>
<td>8 hours</td>
<td>24 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>P3, P4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Change Implementation complete</strong></td>
<td>NTT will complete changes before the end of the change window as mutually agreed upon between client and NTT.</td>
<td>N/A</td>
<td>100%</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

*Table 5 – Service Level Agreements*