

## Managed Detection and Response as a Service (MDRaaS)

### 1 Overview of the Service

NTT's Managed Detection and Response as a Service (MDRaaS) is a turnkey service focused on quickly detecting and effectively responding to cybersecurity threats, using advanced analytics, threat intelligence, expert-driven threat hunting and validation capabilities.

NTT will deploy the MDR platform which includes at a minimum:

- (a) Dedicated log collection points to enable the Client to transmit log data from devices or software within the Client's environment to the MDR Platform.
- (b) A repository for logs with 90 calendar days' retention unless extended storage has otherwise been agreed in the SOW.
- (c) An automation engine for ingesting the log data containing the rules, playbooks and workbooks which provide MDR Incident Alerts to support the security analysts in delivering the MDR Incident Reports to the Client.

#### 1.2 Connectivity Options

Client data sources will send logs and events to MDR platform via one or more of the following connectivity methods which must be determined one time during the Transition Process as agreed by NTT and the Client or otherwise the Connectivity Option is out of scope:

- (a) Direct: HTTPS - Azure API Apps
- (b) Tunneled: VPN - IP Sec Tunnel
- (c) Routed: Azure VNET Peering


### 2 Client Responsibilities


- (a) Client will configure all in scope devices in accordance with the requirements of the Service and NTT instructions, unless specified otherwise in the SOW.
- (b) Client will ensure that all logs from in scope devices, not managed by NTT, are sent to the MDR service platform.
- (c) Client will provide connectivity API keys to log source and device connection.
- (d) Client will install and configure any additional Syslog Forwarders required within their estate. "Additional" to be defined as On-Prem, Client systems or other public cloud for example AWS, specifically excluding Azure, unless otherwise specified in the SOW.
- (e) Client will provide access, as required, to their network or other required assets for the purposes of Digital Forensics and Incident Response (DFIR).
- (f) Client will delegate authority to NTT engineers to contact the technology vendor or any other Client vendor directly and provide any required licenses, use rights and access to NTT.
- (g) Client will provide all authorization, use, rights, licenses or as otherwise required by NTT.
- (h) Client must comply with NTT's MDR Supported Technologies list for ingest, which may be updated by NTT from time to time.
- (i) Client must complete a Response Action Agreement before NTT will perform a Response Action. In the event, no Response Action Agreement is completed by the Client and accepted by NTT, no Response Action will be taken by NTT.
- (j) Client will be responsible for maintaining an authorized list of users and/or a distribution list for notification of MDR Incidents detected by the MDR service. Client will be deemed to have accepted notification of an incident upon NTT's notification to the agreed recipients.
- (k) Upon notification of an MDR Incident by the MDR service, the Client is responsible for activities associated with triage, investigation, and security incident management in accordance with the recommendations provided by NTT in the MDR Incident Report.
- (l) Where NTT is responsible for operational management of a CI which requires remediation as part of the security incident or MDR incident response, Client is responsible for coordinating overall incident response, including raising appropriate incidents and/or Service Requests with NTT, unless mutually agreed in a SOW for support to be provided for the CI.
- (m) Client will log Requests for NTT to provide DFIR service support where the Client would like NTT to provide DFIR services related to a Client Security Incident. Refer to DFIR service scope as defined within section 3 (Service Specific Operations).

























### 3 Service Specific Operations

NTT offers three Service Tiers for MDRaaS. The Service Tier must be selected as In Scope in the SOW, otherwise all are out of scope.

Tasks legend:

(a) Tasks marked as  are included in the service for the specified Service Tier.

(b) Tasks marked as  are not included in the service for the specified Service Tier.

Task	Description	Silver	Gold	Platinum
Ingest Data from Log and Event Sources*	Support the ingestion of data from a range of technologies and services as log and event sources as provided by NTT from time to time. Monitor log feed for log ingestion failure.			
Data Retention	Retain Analytics Logs for in scope devices for ninety (90) days from the date of transmission to NTT. Retain Alert and Incident data for 18 months from the date of creation.			
MDR Incident Detection	Provide 24 x 7 MDR incident detection. Alerts created by the MDR platform, based on the severity of the alert a ticket will be logged in NTT ITSM with a notification to Client, upon NTT's determination in its sole and absolute discretion that an alert requires a ticket.			
MDR Incident Report	Provide Client with a MDR Incident Report that includes a detailed description of the threat, identified activity combined with a recommendation of suitable incident response steps to take. Further updates to the MDR Incident are updated on the Services Portal.			
Information Security Manager (ISM)	Provide a subject matter expert in cyber security, with a strong operational focus ensuring value realization of the MDR service. The ISM supports Client as part of a long-term relationship which enables the ISM to develop a deep understanding of the Client's environment and business. ISM support includes: <ul style="list-style-type: none"> <li>MDR incident escalation point</li> <li>Major incident support between NTT and the Client</li> <li>Optimization recommendations</li> </ul>			
Monthly Service Report	Provide Client with a monthly service report which include extracts from Sentinel Workbooks, Services Portal Widgets, and ITSM incident summary.			
Monitoring	NTT shall monitor the health of deployed system components using native and 3rd party tooling, which shall include at a minimum heartbeat functionality of the agent installed on syslog forwarders in order to ensure at regular intervals of at least every 30 minutes the system is alive (unless otherwise agreed with the Client). NTT will perform remediation actions or escalate to the appropriate vendor if NTT is unable to resolve the issue in a commercially reasonable amount of time.			
Response Action	A Response Action will be performed if the following are met: <ul style="list-style-type: none"> <li>The technology that requires the Response Action has the capability of NTT performing the action;</li> <li>NTT has been granted the appropriate access by the Client;</li> <li>Client has completed the required consent and documentation; and</li> <li>NTT has detected an MDR Incident in its' sole and absolute discretion that requires a Response Action.</li> </ul> Otherwise, all Response Actions are out of scope. A Response Action for a Client under this Service Description shall be limited to restriction on the flow of traffic			

	through a device which manages traffic through the environment.			
Digital Forensics and Incident Response	<p>Provide up to twenty-five hours of DFIR support per contract year, which includes the following:</p> <ul style="list-style-type: none"> <li>• 24 x 7 on-call service</li> <li>• 4-hour Contact Response</li> <li>• Provide remote support and coordination with security and/or IT staff and management to accomplish incident response activities</li> <li>• Provide expert guidance on eradication and recovery</li> <li>• Correlation analysis across various supported and unsupported log sources</li> <li>• Evidentiary compliant handling with chain of custody</li> <li>• Forensic data storage up to 30 days, which shall be in one of the following: Australia, America or the United Kingdom.</li> <li>• Expert digital forensic imaging and analysis on most platforms including mobile, at NTT's sole and absolute discretion</li> <li>• Memory forensics</li> <li>• Review and analysis of various Attack Sensing and Warning (ASW) technologies and related log and network data applicable to the active threat in the environment</li> <li>• Malware reverse engineering</li> <li>• Provide final DFIR report including timeline and analysis findings and recommendations</li> <li>• NTT may provide endpoint detection response tools temporarily to support DFIR investigative activities upon agreement of any required End User License Agreements.</li> </ul>	✓	✓	✓
Use Case Tuning	Tune existing Use Cases for supported sources, to reduce false positives, based on emerging threats, updates to the watchlist and results from threat hunting.	✓	✓	✓
Quarterly Service Review Meeting	Client meetings with ISM to review monthly reports and discuss overall service performance and discuss additional features and roadmap for client.	✗	✓	✓
MDR Incident Management	24 x 7 security analysts validate and investigate threats, suspected threats and notify Client through the Services Portal. NTT may contact Client by telephone for Severity 1 or Severity 2 MDR Incidents. Where applicable, the security analyst will initiate a Response Action.	✗	✓	✓
Check Event Distribution	Compare data source event distribution against historical trends. Associate specific changes linked to seasonal events. Identify risk impact on the Client and provide the ISM with a breakdown of the events.	✗	✓	✓
Threat Hunting	Security analyst proactively and iteratively search through logs to detect and isolate advanced threats that evade existing use cases and existing security solutions using threat intelligence data.	✗	✓	✓
Custom Use Case Tuning	Create Client custom detection rules (up to 10 per year) for specific cases based on Client requirements as deemed reasonable by NTT in its sole discretion.	✗	✗	✓
Targeted Threat Hunting	Investigate and identify patterns on data collected for a specific industry or region (up to 24 per year and no more than 2 per month). Security Analysts review and analyze logs in the LAW and conduct comparisons against new threats and industry specific threats, hunting for any anomalies in a client's environment.	✗	✗	✓

Update Special Handling Notes	Quarterly update special handling notes for Client Security Incident Notification and Management.	✗	✗	✓
-------------------------------	---	---	---	---

\*The table below defines the data ingest commitment rates available within MDRaaS. The Client selected data ingest commitment rate is detailed in the Fees section of the SOW.

Minimum Commitment (GB/day)
10 GB
25 GB
50 GB
75 GB
100 GB
125 GB
150GB
175 GB
200 GB
225 GB
250 GB

#### 4 NTT Services Portal

The MDR platform integrates with the provided NTT Services Portal and allows the Client to view interrogate and leverage MDR dashboards and MDR incident reporting. Select dashboards, information and alerts may be linked to or provided within the Client Azure Tenant. NTT reserves the right to update the NTT Services Portal and provide additional functionality in the future using either the Azure Tenant or a Third Party Provided Application which shall provide at least substantially similar or enhanced functionality.

#### 5 Optional Extended Log Management Services

Client must expressly select Extended Log Management Services in the SOW as in-scope otherwise they are expressly out of scope.

- (a) Log Analytics Workspace Data Retention up to two years.
- (b) Log Analytics Workspace Data Archive up to seven years.
- (c) In the event that no extended Log Managed Service is selected, NTT will determine the retention time of log sources in its sole discretion.

#### 6 Information Security Management

Information Security Management is a component of NTT's MDRaaS delivered by a designated individual. The key functions of Information Security Management include:

- (a) Interpret MDR security information potentially to identify trends and make recommendations.
- (b) Support appropriate business, security, and technical reviews as part of the regular Service Management cadence as detailed below in Coverage.
- (c) Support for Severity 1 and Severity 2 MDR Incidents and provide recommendations on response options up to the provided limits Coverage section.

The primary responsibilities of the Information Security Manager (ISM) include:

- (d) Advise on service optimizations through additional log sources, feeds and intelligence as required to maintain Client service quality.
- (e) Perform reviews of the MDR service against Client security objectives annually.
- (f) Function as final escalation point for technical service-related issues and MDR Incidents requiring additional support after the standard ticket process has been followed.
- (g) Engage with other NTT security teams as required (e.g., MDR Incident Response, Digital Forensics and Incident Response, Cyber Threat Intelligence and Threat Vulnerability Management).
  - (i) Review alerts and advisories from NTT and other Threat Intelligence sources to determine the applicability of the vulnerability to Client's environment and provide advice on actions.
  - (ii) Provide potential security insights and recommendations based on evolving threats.
  - (iii) Form part of escalation team for technical escalations during Business Hours.

## 6.2 Coverage

The availability of Information Security Management (ISM) is subject to applicable locations and shall be the local time zone the Registered Office location of the SOW Signatory of the Client, unless otherwise specified in the SOW.

## (a) ISM Tasks included in the Silver Service Tier

Task	Description	Frequency	Limitations/Out of Scope
Service Delivery Reports	Provide security and technical input to monthly reports required for service delivery.	Monthly	Standard reports only
Client Major Security Incident Management Support	Provide a technical point of escalation for major security incidents identified by the service or escalated and declared by the Client with the Major Incident Management processes operated and managed by the Client.	As needed	During Client local business hours
Service Optimization	Provide expertise to support the optimization of service delivered to Client, working with teams on rule improvements, notification simplification and technical advisories.	As needed	No Client customizations

## (b) ISM Tasks Included in the Gold Service Tier

All of the above tasks included in *Silver*, plus the following:

Task	Description	Frequency	Limitations/Out of Scope
Proactive Solution Health-check	Validate service inputs, confirm efficacy of systems, rules, alerts and outputs against Client business requirements.	Monthly	
Service Improvements and Recommendations	Improvement or recommendations of additional log sources that will provide additional benefit to the Client service based on business requirements.	Monthly	
Security Incident Management	Support Client on security incidents requiring additional expert help from security teams.	As needed	
Service Delivery Reviews	Support monthly service review with the Service Delivery Manager to provide security expert support.	Monthly	All shall be provided remotely
Technical Security Service Analysis	Identify potential technical improvements in the service that can be applied within the bounds of the procured service tier. Recommend additions or updates and, if required, suggest next service tiers as appropriate.	Quarterly	All shall be provided remotely

## (c) ISM Tasks Included in the Platinum Service Tier

All of the above tasks included in *Silver* and *Gold*, plus the following:

Task	Description	Frequency	Limitations/Out of Scope
Custom Use Case Tuning	Work with Client to tune any included custom use cases from the Service.	Monthly	Maximum 5 use cases per month
Targeted Threat Hunting Support	Work with Client and security teams to define scenarios for targeted threat hunting. Work with investigating teams on active threat hunts by providing Client-specific knowledge and expertise.	Monthly	
Service Delivery Reviews	Attend monthly service reviews with the Service Delivery Manager.	Monthly	Option for on-site support with additional costs.

Detailed Insights Report	Threat	Provide detailed security reports to include: <ul style="list-style-type: none"> <li>• Industry insights</li> <li>• Threat landscape information</li> <li>• Risk assessment based on detailed analysis based on anomalies detected in the reporting period</li> <li>• Security insights</li> <li>• Updates on current incident notifications</li> <li>• MITRE mapping of controls and efficacy versus Client targets</li> <li>• Innovation recommendations</li> </ul>	Monthly	
--------------------------	--------	---	---------	--

## 7 Supported Devices for Log Ingestion

NTT maintains a MDR Supported Technologies list for log ingestion which may be updated from time to time by NTT. As part of this Service, only technologies in this list can be supported. This list can be provided on request.

## 8 Limitations

- Response actions can only be performed against supported and in scope technologies, which may be updated by NTT from time to time.
- The twenty-five hours of DFIR incident response that expire at contractual anniversary. Any additional hours during a DFIR incident declared by the Client shall be billed at NTT's current rate or rate card provided in the SOW and updated as allowed by the Agreement. The Client may elect to use unused unexpired DFIR hours for (or as a contribution towards): Incident Response Plan development, Incident Response Plan gap assessment, Incident Response plan testing, Digital Forensics and Incident Response training or Compromise assessment.
- NTT cannot ingest Azure Log Sources that require connection to a Client AD or crossing a Client AD.

## 9 Out of Scope

- Standard Security Services as defined in Client Service Description - Security and Compliance do not apply and are out of scope
- Any activity not specified as in scope.
- Any remediation activities post isolation or containment.
- Any DFIR investigation that exceeds the included 25 hours.
- Configuration of any Client devices.
- Consumption of customized log sources
- Development of customized rules or use cases.
- Creation and presentation of customized reporting
- Individual Device (Policy) Management
- Continuous management of Client incidents including coordination of third parties
- Any device not listed on NTT's supported device list as updated from time to time.

## 10 Tasks Included in the Standard Transition

As part of the Service, the following tasks are included within the setup fee:

- Assign ISM and SDM for the Client and assign to delivery team, if applicable as specified in the SOW.
- Coordinate with Client to schedule the Project Kick-Off Meeting.
- Verify the Client is configured appropriately within each service-dependent system (MS Azure, ServiceNow, CMDB, Nebula, CI/CD, etc).
- Deploy Sentinel, Log Analytics Workspace, LogicApps, Syslog Forwarder and other required Security products as required for the Client Service delivery at the time of the Standard Transition.
- Apply default Project Artifacts (workbook templates / playbooks / analytics rules from CI/CD).
- Provide Client access to MS Azure and guidance for onboarding log sources.
- Confirm all expected log sources are online.
- Perform Normalization and Tuning and any Pre-Go-Live checks.
- Handover to SOC and Service Commencement on agreed date.

## 11 Tasks not Included in the Standard Transition

The following tasks are not included in the standard transition:

- (a) Setup and configuration of any technology or third-party service not in scope of the Services.
- (b) Setup and configuration of any technology or third-party service not defined specifically within Client supplied in scope sources and assets.
- (c) Any setup and configuration of any technology or third-party service that requires physical access to the log source or assets to complete the deployment tasks.
- (d) Any setup and configuration of any technology or third-party service not on NTT's MDR Supported Technologies list as updated from time to time.

## 12 Service Specific Terms and Conditions

The following terms and conditions apply to this Service Description and any dependent thereon, and specifically supersede any conflicting terms and conditions in any other agreement between the parties.

- (a) Client warrants that it has obtained all consents necessary for the data to be collected and used on its behalf for MDR service and that it has a legal basis for requesting such information (excluding consents from NTT employees and agents) and shall indemnify, defend and hold harmless NTT for the use of this information for this Service.
- (b) If Client exceeds the daily ingest threshold in scope in the SOW for three days in a single month, NTT reserves the right to change Client commitment rate. NTT shall make commercially reasonable efforts to notify the Client when the Client has exceeded the commitment rate.
- (c) If Client exceeds the monthly ingest limit (minimum commit x number of days in month < actual ingest), the client will be billed for each additional GB ingested at the rate specified in the SOW.
- (d) In any month that the Client exceeds the daily ingest threshold in scope in the SOW, no Service Level penalties shall apply.
- (e) Client expressly agrees to:
  - (i) Prevent unauthorized access to or use of Services and notify NTT promptly of any such unauthorized access or use;
  - (ii) Use the Services only in accordance with this Service Description, the Documentation, the SOW, Contract, and the Agreement;
  - (iii) Represent and warrant the accuracy, quality and legality of Client Data, the lawful means by which Client acquired Client Data, and Client's right to use Client Data with the Services;
  - (iv) Represent and warrant (i) the provided IP addresses and In Scope Devices and any other devices functioning at those IP addresses are owned or controlled by Client, and (ii) Client has the right to authorize Supplier to access the IP addresses and devices in providing the Services;
  - (v) Not sell Client resell, sub-license, sell, distributes, or transfer the use of the Services to any other party and
  - (vi) Consent to NTT (a) retaining archival copies of work product and (b) using and disclosing general statistics and non-identifiable information regarding vulnerabilities and security issues.
- (f) NTT shall only be responsible for security to systems and Client Data upon which NTT has sole access and control. NTT shall not be responsible for any Client Data stored on Client systems, transmitted to or from third parties, or processed by any third party.
- (g) In the event the Client completes the required documentation to enable disabling of systems to allow NTT to respond to select discoveries made through the Service, Client expressly allows NTT to disable, shutdown or otherwise stop the functionality of any device in scope for this Service and waives all claims for any and all damages related to that activity.
- (h) Client is responsible for backing up all Client Material and Hosted Data. Log files and Sentinel content (including but not limited to workbooks, playbooks, and analytic rules) stored as part of the Service will be immediately deleted by NTT on termination of the Services, and these shall not be returned to the Client. No retention of any Client Materials or Client Data shall be included in this SOW beyond termination, upon termination of this SOW Client shall have 7 days to retrieve any log sources stored in the MDR platform using the process prescribed by NTT.
- (i) NTT shall own all rights, title and interest to any Work Product, Intellectual Property, code or otherwise, developed as part of this Service. In the event Client provides any ideas, suggestions, improvement, Work Product, Intellectual Property, code or otherwise as a suggestion, improvement or otherwise required to enable this Service, Client hereby assigns all rights, title and interest to NTT. Client expressly agrees to the use of Third Party and Open Sources components and services in this Service and agrees to abide by all required terms and conditions of any third-party product. NTT in its sole and absolute discretion may allow Client access to select code upon Client's agreement to NTT's Code License.
- (j) No Control Rule compliance will be included in this Service. This Service Description and Service may be cancelled at any time, in NTT sole and absolute discretion. NTT reserves the right to replace, change, alter, or not provide any third-party software required to perform the Services and any Service that depends on those items may be terminated by NTT.

- (k) MDR Incident shall mean an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies for a Client System connected to the MDR Platform by providing an ingestion feed.
- (l) A MDR Report shall mean a report based on an MDR Incident.

### 13 Third Party Required Terms

1. **Definitions.** The following terms and their variant forms, as used in this Service Description, have the meanings given below:
  - a. "Applicable Laws" mean any court judgement or statute, by-law, directive, treaty, regulation, rule or policy issued by a regulatory authority which:
    - i. in the case of NTT, is applicable to such party's procurement of the third-party technology of the MDRaaS Service; and
    - ii. in the case of Client, is applicable to such party's access and use of the MDRaaS Service
  - b. "AUP" means the acceptable use policy, fair use policy or service use policy (if any) applicable to the MDRaaS as set out in the Microsoft Terms and the fair use policy provided by NTT.
  - c. "Documentation" means user guides and other related documentation for the MDRaaS that NTT makes available to Client.
  - d. "Intellectual Property Rights" mean any of the following rights anywhere in the world, whether registered or unregistered: patents and application for patents, trademark rights, service mark rights and domain name rights and applications for the same, rights in unregistered trademarks and rights in trade names and business names, copyright (including copyright in software and databases), database rights, rights in designs and rights in inventions, and any rights of similar effect or nature as any of the foregoing.
  - e. "MDRaaS" means the Microsoft Azure Services and services provided under this Service Description Provided to Client.
  - f. "Microsoft" means Microsoft Corporation or its affiliates or subsidiaries from which NTT procures the Microsoft Azure Services.
  - g. "Microsoft Azure Services" means the Microsoft services which NTT makes available to Client under this Service Description. "Microsoft Azure Services" includes any opensource components incorporated by Microsoft in those services and features.
  - h. "Microsoft Data Protection Addendum" means the data protection addendum or other privacy terms applicable to Microsoft's provisioning of the Microsoft Azure Services, as set out further in the Online Services Terms.
  - i. "Microsoft Enrollment Agreement" means the Microsoft server and cloud enrollments (including all agreements and amendments to which they are subject and/or any documents or supplemental terms incorporated therein) entered into by NTT and Microsoft for the purpose of obtaining the Microsoft Azure Services, as contemplated by this Service Description.
  - j. "Microsoft Terms" means the Online Services Terms and Product Terms.
  - k. "Online Services Terms" means, as published by Microsoft at the Volume License Site, the Online Services Terms and all additional terms or documents incorporated therein (including, without limitation, the Microsoft Data Protection Addendum), which set out the use rights and terms of service for the Microsoft Azure Services. For the purposes of the Microsoft Azure Services, the term "Online Services Terms" will have the same meaning as "Use Rights" (as used in the Microsoft Terms).
  - l. "Personal Data" means any information relating to an identified or identifiable person or other similar definition under any Applicable Laws governing treatment of personal information or data.
  - m. "Product Terms" means the document published by Microsoft at the Volume Licensing Site that provides information about the Microsoft Azure Services.
  - n. "NTT Material" means: (a) the Services and associated Documentation; (b) equipment (including associated firmware, software, parts and components) leased, rented or licensed by or on behalf of Secure-24 in order for Customer to receive and use any Services, regardless of physical location; know-how, methodologies, processes, and/or Intellectual Property Rights used by NTT to provide any Microsoft Azure Services; (d) all materials, software, data and information provided by NTT under a contract, including any identifiers, passcodes or access keys used to access the Services; and (e) any modifications, upgrades, derivative works and improvements to any of the foregoing.
  - o. "Volume Licensing Site" means <http://www.microsoft.com/licensing/contracts> or a successor site.
2. **Third Party Software**
  - a. NTT will provide the Microsoft Azure Services to Client (subject to the terms of the Microsoft Enrollment Agreement) as part of a MDRaaS solution only. Hereinafter MDRaaS shall include both the Microsoft Azure Services and the Services provided under this Service Description.
  - b. Subject to the terms of this Service Description, Client is granted, during the Service Description Term only, a non-exclusive and limited right to access and use the Microsoft Azure Services for internal business use only as part of MDRaaS provided by NTT. The rights granted in this clause are non-transferable except as expressly permitted under this Service Description or Applicable Laws.
  - c. Client expressly agrees to be bound by the Microsoft Terms.
  - d. **Reservation of Rights.** The MDRaaS Service is licensed and not sold and are protected by copyright and other intellectual property laws and international treaties. No Intellectual Property Rights are intended to be transferred under this Service Description. All rights not expressly granted in this Service Description are reserved by NTT (on behalf of itself or, as applicable, Microsoft).
  - e. **General Restrictions.** Client must not (and is not licensed to):
    - i. reverse engineer, translate, decompile or disassemble the MDRaaS Services;

- ii. use Documentation for any purpose other than as strictly necessary for Client to receive the intended benefit of the MDRaaS Service;
  - iii. remove, obscure or alter any trademarks or other proprietary notices appearing on or contained within any material supplied by NTT or Microsoft;
  - iv. use the NTT Material (or any part), the MDRaaS Service in any manner that violates: (a) the terms of the applicable AUP (if any); or (b) Applicable Laws;
  - v. work around any technical limitations or restrictions applicable to the MDRaaS Services, or Documentation;
  - vi. distribute, resell, sublicense or otherwise transfer the MDRaaS;
  - vii. use the MDRaaS in any manner that is otherwise inconsistent with the Microsoft Terms; or
  - viii. Use the MDRaaS s separately or not part of the MDRaaS service.
- 3. **Privacy and Compliance with Laws**
  - a. Client consents to the processing of Personal Data by NTT and Microsoft (as well as such parties agents) to facilitate the subject matter of this Service Description. Client hereby grants all required consents from third parties (including, but not limited to, administrators, users' employees or Clients, as applicable) under Applicable Laws before providing Personal Data to NTT and Microsoft.
  - b. Client acknowledges that Personal Data collected under this Service Description: (a) may be transferred, stored and processed in the United States or any other country in which NTT, NTT's supplier or Microsoft (or their service providers) maintain facilities; and will be subject to the privacy terms as more particularly set out in 3c, and 3d.
  - c. Processing by NTT. Excluding any Personal Data processed by Microsoft in connection with Client's use of the Microsoft Azure Services, which will be subject to the terms set out in clauses 5d. below, the parties respective rights and obligations in relation to any Personal Data processed in connection with this Service Description will be in accordance with the Data Process Agreement in place between the parties. The Privacy Terms are incorporated into this Service Description by the reference in this clause.
  - d. Processing by Microsoft. The parties respective rights and obligations in relation to any Personal Data processed by Microsoft in connection with Client's use of the Microsoft Azure Services will be subject to the privacy terms set out in the Online Services Terms (including, as applicable, the Microsoft Data Protection Addendum).
  - e. Client agrees its use of the Microsoft Azure Service shall be in compliance with all Applicable Laws.
- 4. **Indemnities**
  - a. Client Indemnity. Client will defend and indemnify NTT (and its directors, officers, employees and contractors) from and against all third party claims (including, for the avoidance of doubt, any claim initiated by or on behalf of Microsoft) arising out of Client's (a) Customer Data, (b) the Client Material, Client Data transmitted or used by, through or on behalf of NTT in connection with any service provided under this addendum, (c) access or use of the MDRaaS in a manner inconsistent with the terms of this Service Description, or (d) Clients failure to comply with the obligations of section 2 or 3 above.
- 5. **Additional Termination Rights**
  - a. NTT may terminate this Service Description (and any other agreement, complete or partial SOW, or any other agreement for services dependent on the continuation of the MDRaaS in NTT sole and absolute discretion) without any penalty or liability for any amount, if there any reason NTT is unable to provide the MDRaaS Service for any reason (including but not limited to a change in the rights of access to the underlying technology), provided NTT will provide Client with as much prior notice of such termination as is reasonably possible under the circumstances. Upon which all access to these services under this Service Description shall terminate.
- 6. **Updates to Service Description**
  - a. Modifications to or Termination of MDRaaS
    - i. Client acknowledges and accepts that NTT may modify the MDRaaS Service Description or these terms at any time, subject to the applicable third party terms. Such modifications may include the release of a new version, addition of new features or functionality, or changes to or removal of existing features or functionality.
    - ii. Without limiting the generality of clause 6 (a) (i) above, NTT may modify or terminate the MDRaaS Services in any country or jurisdiction where there is any current or future government requirement or obligation that:
      - 1. subjects NTT or a third party to any regulation or requirement not generally applicable to businesses operating there;
      - 2. presents a hardship for NTT to continue to operate the MDRaaS without modification; or
      - 3. causes NTT to believe the terms of which it acquires the underlying service structure may conflict with any such requirement or obligation.
    - iii. NTT has no liability in relation to, any such changes to or termination of the MDRaaS Service including where any such changes would result in additional Fees or cause a detriment to Client.
  - b. Updates to the MDRaaS Terms - Client acknowledges and accepts that third parties directly maintains and may update or revise the third party terms at any time. Any such update or revision to the third party will be effective pursuant to the terms set out therein (without any further action by NTT)
  - c. Updates to the Service Description Terms - Client acknowledges and accepts that the agreements which NTT is using to obtain the services may be unilaterally altered and any such alterations will automatically apply to this Service Description. NTT will try to provide as much notice as possible for any changes which may materially impact this Service Description.
- 7. **Miscellaneous**

- a. Disclosure of Information. Client consents to NTT providing Microsoft and other third parties with information relating to Client's use of the MDRaaS, including (without limitation) relevant contact information and information regarding any known or suspected breach of the Microsoft Terms.
- b. Verifying Compliance. Client acknowledges that Microsoft reserves the right to verify compliance with the license terms applicable to the MDRaaS. Client must promptly assist NTT, Microsoft and/or Microsoft's independent auditor with any such review, as reasonably instructed by NTT or Microsoft. For the avoidance of doubt, any request for assistance that is in accordance with the mandated terms of the Microsoft Enrollment Agreement between NTT and Microsoft will be deemed reasonable under this clause (b). In the event NTT incurs any damage or cost as a result of Client's non-compliance, as determined by the review set out in this clause, Client will indemnify NTT for such damage or cost in accordance with clause 9 (a)
- c. U. S. Export. Aspects of the third party solution of MDRaaS are subject to U.S. export jurisdiction. Client must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulation, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft products, services, and technologies.
- d. Use of Contractors. NTT (or Microsoft) may use contractors to perform services, but will be responsible for their performance, subject to the terms of this Service Description.