dimension data

accelerate your ambition

Together we can
do great things.

Managed Services Agreement

Managed Security Services

Dimension Data
and
Client Name:

If you believe you can do anything,
we're here to help you do it.

Part A. Agreement Details

This section sets out details of the agreement for the supply by Dimension Data Proprietary Limited of the described Services and forms part of this Agreement.

Dimension Data		Client	
Name		Name	
Registration number		Registration number	
Address		Address	
City		City	
State		State	
Post Code		Post Code	
Contact		Contact	
Telephone		Telephone	
Facsimile		Facsimile	
Position		Position	
Email		Email	

Client's Invoice Details					
Attention		Position			
Address		Registration number			
City		Country		Postcode	

Service Details		
Service Packages	☐	Managed Security Services Threat Detection - Standard
	☐	Managed Security Services Threat Detection - Enhanced
	☐	Managed Security Services Enterprise Security Monitoring - Standard
	☐	Managed Security Services Enterprise Security Monitoring - Enhanced
	☐	Managed Security Services Security Device Management - Standard
	☐	Managed Security Services Security Device Management - Enhanced
	☐	Managed Security Services Vulnerability Management

Contract Details	
Initial Term	
Service Commencement Date	

Service Charges – Managed Network Services					
Monthly Charges					
Service Charge Excluding VAT	Rand				
OR	☐	As set out in the Record of Entitlements			

One-Off Charges					
Transition Fee Excluding VAT	Rand				
Audit Fee Excluding VAT	Rand				
Number of MACD Service Unit bundles included		50 MACD Service Units			
Total MACD Service Unit bundle charge Excluding VAT	Rand				

Service Desk and Service Portal Details	
Service Desk Telephone Number	
Service Desk Email Address	
Service Portal URL	

Dimension Data		Client	
Signed on behalf of Client by:			
Name		Position	
Signature		Date	
Signed on behalf of Dimension Data by:			
Name		Position	
Signature		Date	

Table of Contents

Part B. Definitions and Interpretations

1. Definitions

1.1 For the purposes of this Agreement, unless the context requires otherwise:

"**Additional Charge**" means a charge payable by Client to Dimension Data for the supply of any Services other than the Services, made at Dimension Data's then current standard prices and rates unless otherwise agreed in writing between the Parties.

"Affiliate" means:

a. in relation to Dimension Data, any business entity, which at the time of any applicable transaction under this Agreement, is (either directly or indirectly) owned by, or is under common ownership by Dimension Data; and

b. in relation to Client, any business entity, which at the time of any applicable transaction under this Agreement, directly or indirectly owns, is owned by, or is under common ownership of Client.

"**Agreement**" means this document, the relevant Record of Entitlements and agreed variations of them but excludes any term and conditions attached to or referred to in the Client's purchase order(s).

"**Agreement Details**" means the details set out in the section of this Agreement so named.

"Anti-Bribery Laws" means applicable anti-bribery and corruption Laws.

"Attribute" means an item of information recorded about a Configuration Item.

"Availability Plan" means a plan in terms of which the current availability of Client's infrastructure is assessed against Client's future infrastructure availability requirements.

"**Business Day**" means a day other than a Saturday, Sunday or a public holiday in the state or territory in which the Service is to be supplied.

"Capacity Plan" means a plan in terms of which the current capacity of Client's infrastructure is assessed against Client's future infrastructure capacity requirements.

"Change Advisory Board" means a formalised body that supports the assessment, prioritisation, authorisation, and scheduling of changes and comprises Client and, if applicable, Dimension Data representatives.

"Change Plan" means a plan used to streamline the change management process developed to the extent appropriate for the type of change being undertaken. A change plan may include a change impact analysis report, change communication plan, change implementation plan, change test plan, and a change rollback plan.

"**Client**" means the Party specified as such in Part A. Agreement Details.

"Client Material" means material owned or developed by or for Client independently and outside of this Agreement and furnished by Client for use by Dimension Data in connection with the Services, and which includes information, documentation, designs, specifications, instructions, data and software, but specifically excludes Third Party Material.

"**Change Request**" means a request generated by the Client or Dimension Data for the addition, modification, or removal of anything that could have an effect on a Configuration Item and/or the provision of the Services.

"Confidential Information" means any confidential business and financial information of a Party including, without limitation, information concerning the business operations and methods of a Party or technical information acquired either directly or indirectly by the

other Party but excludes information which is or becomes publicly known through no wrongful act of the Receiving Party and for the removal of doubt it includes the relevant Scope of Service.

"**Configuration Item**" means any item of Hardware or Software listed in the Record of Entitlements unless identified as a spare.

"Consulting and Professional Services" means such activities as analysis, planning, architecture, development, consulting, implementation, installation, training, project management, and such other similar activities.

"Data Controller" means Client, who alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

"Data Processor" means a Dimension Data entity or Third Party which Processes Personal Information on behalf of Client.

"**Dimension Data**" means Dimension Data Proprietary Limited

"Dimension Data Equipment" means equipment owned by Dimension Data or a Third Party which is used in the provision of Services.

"**Dimension Data Management System**" means the system used by Dimension Data to record information relating to the provision of the applicable Services.

"Dimension Data Material" means material owned or developed by or for Dimension Data independently and outside of this Agreement and furnished by Dimension Data as part of the Service and used by Client in connection with the Services, and which includes Dimension Data Software, and information, methodologies, tools, techniques, documentation, designs, specifications, instructions and data, and any modifications thereof, but specifically excludes Third Party Material.

"Disclosing Party" means any Party or its Affiliate disclosing Confidential Information under this Agreement.

"**End-of-Life**" means the relevant Configuration Item is no longer manufactured or supported, as determined by Dimension Data, based on any end-of-life or end-of-service announcements made by the Manufacturer.

"Emergency Maintenance" means any non-scheduled, non-standard maintenance required by Dimension Data.

"**Event**" means systematic detection or correlation of one or more Logs that identifies activity of interest.

"**Force Majeure Event**" means any event beyond the reasonable control of a Party, including but not limited to acts of God, changes in Laws, earthquakes, acts of war or public enemy, terrorism, strikes, applicable trade sanctions, acts of sovereign states, blockade, embargo, quarantine, banking sanctions, public disorder, cable cuts, power outage, sabotage, accident, or any similar events which impact on that Party's ability to perform its obligations.

"Good Industry Practice" means standards, practices, methods and procedures conforming to the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person engaged in a similar type of undertaking under the same or similar circumstances.

"Governing Law State" means the state or territory specified as such in *Part A. Agreement Details*.

"Hardware" means computer equipment and other goods and any substitute or additional equipment, products materials or component parts as agreed between the Parties.

"Initial Term" means the first term of the Agreement, being the period specified as such in *Part A. Agreement Details*.

"Intellectual Property Rights" means any of the following rights anywhere in the world, whether registered or unregistered:

a. any patents and applications 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

b. any rights of a similar effect or nature as any of those in paragraph (a) of this definition.

"**Law**" means any statute, by-law, directive, treaty, regulation, or court judgement, and any rule or policy issued by any regulatory authority.

"Location" means any location at, or from which, the Services are to be provided, as specified in *Part A. Agreement Details*.

"Log" means a record of activity generated by a system or application.

"**MACD Service Unit**" means a prepaid unit of credit purchased by Client from Dimension Data that is used to pay for specific activities on a consumption basis.

"Manufacturer" means either the original equipment manufacturer or the owner or licensor of the Software, as applicable.

"Next Business Day" means the same time on the next Business Day as the Client logged the relevant Security Incident, Change Request or Service Request on a Business Day.

"Party" means Client or Dimension Data or their successors and permitted assigns.

"**Permanent Resolution**" means the action taken to resolve the root cause of a Security Incident or Problem.

"Personal Information" has the meaning set out in the Protection of Personal Information Act 4 of 2013.

"Point of Contact (POC)" means Client personnel designated for communication with Dimension Data.

"**Priority**" means the relative urgency and importance of an Event, Security Incident, Problem, Change Request, or Service Request based on a combination of impact and urgency, with Priority 1/critical being the highest and Priority 5/low being the lowest.

"**Problem**" means the cause of one or more Security Incidents.

"Process or Processing" means any operation or set of operations performed in respect of personal data, whether automated or not, including collection, recording, transfer, utilisation, adaptation or alteration, retrieval, disclosure and storage of Personal Information, by transmission, dissemination, or any other means of making it available.

"Receiving Party" means any Party or its Affiliate receiving Confidential Information disclosed under this Agreement.

"Record of Entitlements" means the document issued by Dimension Data at the Service Commencement Date, and re-issued from time to time, which sets out details of the

Configuration Items, Service Calendar, Service Level Targets, Service Charges, options and other relevant details.

"Security Incident" means an Event or threat in Client's environment detected by the Service.

"Security Incident Diagnosis" means the performance of an investigation (not remediation) by Dimension Data into the possible causes of a Security Incident.

"**Security Incident Record**" means a record in Dimension Data's Management System generated either by the Client or Dimension Data that records and tracks a Service Request related to a Security Incident.

"Security Incident Report" means a report, prepared by a Dimension Data security analyst that details a Security Incident detected in Client's environment.

"Security Operations Centre (SOC)" means Dimension Data facilities staffed with personnel qualified to receive, analyse, and respond to Events, and Security Incidents for the Service.

"**Service Calendar**" means the hours and days specified in the Record of Entitlements during which the Service for the applicable Configuration Item is available.

"**Service Commencement Date**" means the date on which Dimension Data commences providing the Services, following any applicable Transition period, as set out in *Part A. Agreement Details*.

"Service Charges" means the charges for the Services set out in *Part A. Agreement Details*, an invoice issued by Dimension Data and/or as detailed in the Record of Entitlements.

"Service Desk" means the Dimension Data technical support group that acts as a single point of contact between Dimension Data and the Client to manage all Security Incidents, Service Requests, Change Requests, communications and escalations with the Client.

"Service Feature" means ITIL-aligned activities that make up a Service Package, identified in the relevant Scope of Service.

"**Service Level Target**" means a commitment that is specified in Part F. Service Level Targets.

"Service Package" means the specific Services purchased by the Client, including but not limited to that set out under the Record of Entitlements, Service Level Targets or as may otherwise be agreed under or pursuant to this Agreement.

"**Service Portal**" means the internet portal created and configured by Dimension Data used for Security Incident workflow, reporting, and document management.

"**Service Request**" means a request generated by the Client or Dimension Data for information or for a Standard Change or for access to an IT service, which are managed by the request fulfilment process.

"**Services**" means the services described in this Agreement.

"**Site**" means the premises specified in the Record of Entitlements at which a Configuration Item is located.

"**Software**" means software listed in the Record of Entitlements or which forms an integral part of a Configuration Item but does not include any software installed on the Hardware by the Client unless it is listed in the Record of Entitlements.

"**Standard Change**" means a low risk, relatively common change that is mutually agreed and documented and constitutes a pre-approved change that is implemented through a Service Request.

"Term" means the Initial Term and any extension of it.

"**Third Party**" means any person who is neither a Party to this Agreement nor an employee of either Third Party.

"Third Party Material" means any Third Party Software and any documentation, including operating manuals, user technical literature or related materials, on any online or offline media, that is supplied, used or made available to a Party in the provision of the Services, but which is not proprietary to either Party.

"Third Party Software" means Software owned by Third Parties that Dimension Data uses or makes available to Client in connection with the Service.

"**Transition**" means any period during which Dimension Data and the Client will perform certain obligations to prepare for and enable the provision of the Services, as set out in this Agreement.

"VAT" – means Value Added Tax in terms of the Value Added Tax Act of 1991.

"**Workaround**" means a set of actions that reduces or eliminates the impact of a Security Incident or Problem for which a Permanent Resolution is not yet available.

2. Interpretation

2.1 In this Agreement:

a. the singular includes the plural and vice versa;

b. a gender includes all genders;

c. if a provision needs to be read down, it must be read down and if a provision cannot be read down, it is deemed void without affecting the remaining provisions;

d. if a court declares that any provision of this Agreement is void, illegal or unenforceable, then to the extent possible, the remainder of this Agreement is to be interpreted or construed to facilitate the operation of this Agreement consistent with the expressed intention of the void provision and any adverse declaration, will not affect or be applied to the provision in a jurisdiction where it is valid;

e. references to currency are references to South African Rand currency;

f. one provision does not limit the effect of another unless otherwise stated;

g. all obligations are taken to be required to be performed duly and punctually, and in a professional manner;

h. headings are for guidance only and do not have any operative effect;

i. unless otherwise stated, this Agreement ensures to the benefit of the Parties and their successors or approved assigns, but not other Parties; and

j. if any provision is capable of continuing operative effect after termination or expiry of this Agreement it will continue to have such operative effect.

Part C. Terms of Service

3. Term and Termination

3.1 The provision of the Services will commence on the Service Commencement Date and, unless terminated earlier in accordance with the terms of the Agreement, shall endure for the Initial Term.

3.2 After the Initial Term (or any renewed Term), this Agreement continues for a further Term of 12 months, unless either Party gives the other Party written notice not to renew this Agreement at least 90 days prior to the end of the Initial Term (or the renewed Term), as the case may be.

3.3 The Service Charges payable for a renewed Term must be the same amount as was payable immediately before expiry of the prior Term, unless varied pursuant to clause 14.8.

3.4 For the avoidance of doubt, the terms that shall apply following any extension 3.3 may differ from those terms which applied immediately prior to the extension, and will be subject to any Service Charges as set out *Part A. Agreement Details*.

3.5 If a Party breaches any provision of this Agreement, the other Party may:

a. suspend provision of the Services or payment of any amounts otherwise due (as the case may be) until the breach is remedied by the Party in breach; and

b. terminate this Agreement, if the Party in breach remains in breach of any such provision after receiving at least 30 days' notice in writing from the other Party identifying the breach and requesting its remedy.

3.6 Either Party may terminate this Agreement immediately if the other Party:

a. enters into any arrangement between itself and its (or any class of its) creditors;

b. ceases to be able to pay its debts as they become due;

c. ceases to carry on business;

d. has a mortgagee enter into possession or disposes of the whole or any part of its assets or business;

e. enters into liquidation or any form of insolvency administration; or

f. has a receiver, a receiver and manager, a trustee in bankruptcy, an administrator, a liquidator, a provisional liquidator or other like person appointed to the whole or any part of its assets or business.

3.7 If Dimension Data terminates this Agreement, Client must immediately pay to Dimension Data the total of all amounts then due to Dimension Data pursuant to this Agreement.

3.8 If Dimension Data terminates this Agreement on any of the grounds set out in clauses 3.5 or 3.6 Client is not entitled to a refund or adjustment of any applicable Transition Fee or of any Service Charges paid to Dimension Data.

3.9 If Client terminates this Agreement on any of the grounds set out in clauses 3.5 or 3.6, Client is entitled to a pro-rata refund of any part of the Service Charges it has paid for Services to be supplied after the date of termination.

3.10 If Client terminates this Agreement before the end of the initial Term (or any renewed Term), Client will attract a termination payment of the minimum monthly Service Charges for the remaining months of the Agreement.

3.11 Termination of this Agreement (for whatever cause) does not affect any right or cause of action which has accrued to the Party which terminates this Agreement at or prior to the date of termination.

4. Services

4.1 During the Term Dimension Data must supply the Services to Client and Client must pay the Service Charges and any Additional Charges.

4.2 Dimension Data will, at its discretion, have the right to make changes to a Service, provided that any such change will not materially alter the Service's features or functionality, and will not result in a material degradation to the Service Level Targets.

4.3 Dimension Data may make adjustments or add enhancements to the Dimension Data Management System during the Term. Dimension Data will provide advance notice of any such changes, where possible.

5. Dimension Data's General Obligations

5.1 Dimension Data must:

a. provide Services to Client;

b. use Dimension Data employees who have appropriate skills and experience for their duties;

c. co-operate with Client and comply with Client's reasonable instructions;

d. perform the Services using reasonable care and skill and in accordance with Good Industry Practice;

e. provide and use sufficient and appropriate equipment and materials required to provide the Services;

f. obtain and maintain all licences, permits and other consents required for its performance of the Services; and

g. comply with all Laws applicable to Dimension Data in the supply of the Services.

6. The Client's Obligations

6.1 The Client must:

a. provide Dimension Data with such access, assistance, information and cooperation using reasonable care and adequate skill as Dimension Data may reasonably request in order to perform its obligations under this Agreement;

b. advise Dimension Data of changes to any of Client-nominated escalation contacts within 48 hours of such changes;

c. supply all communications interfaces Dimension Data requires to enable provision of the Services, except those that Dimension Data keeps on its own premises or installs at a Client Site for use in providing the Services;

d. comply with any reasonable instructions given by Dimension Data;

e. ensure that Dimension Data's information and materials in the custody of Client for the purposes of this Agreement are always protected from unauthorised access or use by a Third Party and from misuse, damage or destruction by any person;

f. ensure that Dimension Data Equipment in the possession of Client is always protected from unauthorised access, misuse, damage or destruction by any person;

g. give Dimension Data access to a Client Site when required for the purpose of providing the Services;

h. provide Dimension Data with remote access to the Configuration Items as required by Dimension Data to provide the Services, including ensuring relevant firewall configuration to allow access and, if required, redundant connectivity;

i. keep all records relating to use and performance of the Configuration Items which are the subject of the Services as Dimension Data may reasonably request and ensure that Dimension Data's personnel have access to such records at all reasonable times;

j. establish and maintain connectivity between Client's equipment, network and/or systems and Dimension Data's Equipment, network and/or systems, as required by Dimension Data to perform its obligations;

k. ensure that Configuration Items are covered by valid Hardware and Software maintenance contracts, with Service Level Targets and response times that align with the Service Level Targets and response times to be provided by Dimension Data;

l. notify Dimension Data through a Service Request of all changes to configuration files, including user access credentials, that will affect Configuration Items and the configuration download, no less than 2 (two) Business Days prior to implementing the change;

m. maintain the integrity of Log files associated with a Configuration Item to enable Dimension Data to fulfil its diagnostic obligations, and if the Event Log files are deleted or modified, Client will incur an Additional Charge for Dimension Data to remediate;

n. review and validate the information stored in the Record of Entitlements and notify Dimension Data of any discrepancies on a regular basis;

o. ensure the correct Software versions are installed on all Configuration Items to enable Dimension Data to retrieve configuration files;

p. promptly notify Dimension Data of any changes it makes to the details relating to a Configuration Item as set out in the Record of Entitlements;

q. comply with all Laws applicable to the receipt of and use of the Services by Client;

r. neither use nor permit the use of the Services in such a way as to cause harm, interruption, interference, impairment or degradation to, or abuse of, any Dimension Data network or system or any Third Party network or system that is used by Dimension Data in the provision of any Services;

s. obtain and maintain all necessary licences, authorisations, permits and consents necessary for its acceptance and/or use of the Services;

t. upon request provide Dimension Data with reasonable evidence that Client has adequate, published guidelines and procedures for occupational health and safety purposes in respect of each Site and that Client has satisfactory public liability insurance cover;

u. complete any Transition tasks and changes to Configuration Items as reasonably requested by Dimension Data to enable the provision of the Services and allow Dimension Data to perform its obligations; and

v. before returning any Configuration Items to Dimension Data, the Manufacturer, or a Third Party as directed by Dimension Data, completely erase the Client's and/or any end users' information and data, including all Confidential Information and Personal Information, from such Configuration Items.

6.2 The Client will indemnify and defend Dimension Data against any and all claims, liabilities, losses, damages, costs and expenses incurred by or asserted against Dimension Data from any consequences of the Client's failure to completely erase the information and data from such Configuration Item.

6.3 If Client fails to promptly comply with any of Client's obligations set out in this Agreement, Dimension Data may, in its absolute discretion, suspend performance of that part of the Services affected as a result of Client's failure or refusal until Client has complied with its obligations.

6.4 If requested, Client must provide Dimension Data with reasonable evidence that Client has adequate, published guidelines and procedures for Workplace Health and Safety purposes in respect of each Client Site, and that Client has satisfactory public liability insurance cover.

6.5 Unless otherwise agreed between the Parties, Client may not sell or resupply the Services to any Third Party.

6.6 Where Dimension Data requires Third Party Material to be made available to it by Client in order to supply the Services, Client must, unless otherwise agreed, obtain at its own cost the necessary licence, consent, authorisation, permission or right of use from the relevant Third Party owner or licensor.

7. Additional Rights and Obligations

7.1 Urgency and classification of all Security Incidents must be agreed by both Dimension Data and Client.

7.2 Dimension Data requires exclusive access to all Configuration Items within scope for the purposes of monitoring the Configuration Items and, where applicable, updating of the Configuration Items.

7.3 Client must notify Dimension Data of availability and capacity requirement changes.

7.4 Configuration Item configuration file backup is limited to the Configuration Items compatible with the Configuration Item file backup Software or platform.

8. Client Equipment

8.1 Client must ensure that any Client equipment, network or systems connected to any Dimension Data Equipment, network or systems and/or used in receiving the Services is technically compatible, connected and used in accordance with any instructions and/or safety and security procedures applicable to the use of such Client equipment or as directed by Dimension Data.

8.2 If any Client equipment, network or systems do not comply with the requirements of this clause 8, Client must advise Dimension Data and upon notice from Dimension Data, disconnect such Client equipment, network or systems and where applicable direct Dimension Data to do the same, the cost of which will be borne by Client.

8.3 Dimension Data will not be liable for any failure to meet any Service Level Target or other obligations set out in this Agreement if the failure is caused by Client's breach of its obligations under this clause 8 or otherwise.

8.4 Dimension Data gives no warranty in respect of the interoperability between the Dimension Data Equipment, network and/or systems and any Client equipment, network or systems.

9. Maintenance

9.1 Dimension Data must perform scheduled maintenance on the Services, including maintenance related to the Software and other equipment and materials used for providing the Services, during maintenance windows notified by Client.

9.2 Dimension Data must notify Client in writing at least 3 (three) Business Days' in advance of any scheduled maintenance, any related Service interruptions and their anticipated durations.

9.3 In the case of Emergency Maintenance, Dimension Data:

a. will endeavor to provide Client with at least 20 minutes' prior written notice;

b. notwithstanding subclause 9.3a, will provide the Client with as much written notice as is reasonably practicable in the circumstances; and

c. use its best efforts to minimise the duration of any interruption or disruption to the Service.

9.4 Dimension Data will be relieved of its obligations under the applicable Service Level Agreement for the duration of the Emergency Maintenance and the Client expressly excludes Dimension Data for any liability, loss and or damage suffered during an Emergency Maintenance period.

10. Remote Management Access Requirements

10.1 Where applicable, Client must configure a virtual private network (VPN) tunnel between the applicable Client data centres and a Dimension Data data centre.

a. Detailed configuration requirements for the VPN, including authentication mechanisms and firewall rules, will be provided by Dimension Data as part of the Transition process.

11. Service Level Target Exclusions

11.1 Dimension Data will not be liable for Service Level Target defaults resulting from one or more of the following events:

a. any of the events specified in the Terms of Service in this Agreement;

b. absence of a patch, repair, policy, configuration or maintenance change recommended by Dimension Data but not approved by Client;

c. scheduled downtime in respect of Dimension Data Equipment (including upgrades, repair or component replacement, or scheduled backups) or any other mutually agreed-to downtime;

d. changes made by Client to covered Configuration Item or protected server configurations where Client has not notified Dimension Data;

e. unavailability of access to a Site;

f. damage or delay arising from Client failing to carry out an action or contractual obligation required by Dimension Data in order for it to render the Services in a timely manner and/or in accordance with the agreed Service Level Targets;

g. time taken for Hardware maintenance vendor to respond, as specified in a Client maintenance agreement;

h. damage to equipment used to render the Services and which are within Client environment by abnormal operating conditions such as high or low temperatures or humidity or dust levels or fluctuations of electrical power, which are beyond the published environmental specifications of the Manufacturer;

i. modifications, repairs or replacements or attempted modifications, repairs or replacements not performed by Dimension Data or not approved by Dimension Data in writing prior to such modifications, repairs or replacements being performed or attempted by any other Party, including the Client;

j. the restoration of any lost data from any products, or devices connected to configuration items, without Dimension Data's knowledge;

k. products where Client has failed to licence such products and such licence is a prerequisite of the Manufacturer or where such licence is no longer current or valid or when such products have been purchased outside of acceptable purchasing norms (commonly referred to as 'grey-market' products);

l. failure of Client Software tools that are used in conjunction with the Dimension Data Management System;

m. data provided by Client is inaccurate or not up-to-date; or

n. a virus, worm, distributed denial of Services, or any other malicious activity.

12. Sites

12.1 The Services are performed remotely and not at a Client Site. Client may request that Dimension Data perform a Service at a Client Site, and Dimension Data may, at its discretion, agree to do so. If agreed by Dimension Data, such obligations will be performed at an Additional Charge, and invoiced in accordance with clause 14.

12.2 Dimension Data may at its sole discretion utilise resources temporarily or permanently located in other Dimension Data locations for the delivery of the Services.

13. Service Desk and Service Portals

13.1 The Service Desk contact details, links and pre-requisites (if applicable), are set out in *Part A. Agreement Details*.

14. Service Charges and Payment Terms

One-Off Charges

14.1 The following Fees will charged as one-off Service Charges:

a. the Transition Fee upon the Service Commencement Date; and

b. a MACD Service Unit Charge when Client has exhausted the number of MACD Service Units included in the pricing.

Recurring Service Charges

14.2 The recurring Service Charges are as set out in *Part A. Agreement Details*.

14.3 Where agreed changes are made to the Record of Entitlements, Dimension Data must invoice the Service Charges for the adjustments pro rata to the end of the then current Term.

Invoices

14.4 Dimension Data will issue invoices for the Service Charges set out in in *Part A. Agreement Details* and must send each invoice to the address specified in *Part A. Agreement Details*

or as Client may otherwise specify in writing. If applicable the invoice for the Transition Fee will be rendered at the commencement of the Term. If Client disputes an invoice in part, it may defer payment of only that disputed part pending resolution of the dispute.

14.5 Dimension Data must issue invoices for any Additional Charges when it has done the relevant work, supplied the Services or incurred the expenses.

14.6 The Service Charges set out in *Part A. Agreement Details* shall become payable by Client from the Service Commencement Date. When the Service Commencement Date is delayed through the fault of Client, Dimension Data shall be entitled to commence invoicing Client for the Service Charges with effect from 60 days after the Service Commencement Date.

Payment Terms

14.7 Client must pay the Service Charges, any applicable Transition Fees and any Additional Charges within 30 days after the date on which Dimension Data's invoice is rendered.

Variation of the Service Charges

14.8 Dimension Data may, by giving at least 30 days' written notice of the variation to Client, vary the Service Charges:

a. at any time after the Initial Term expires;

b. at the end of a renewed Term; or

c. at any time after the first 12 months of the Term, if the Initial Term exceeds 12 months and Dimension Data has, with the Client's consent subcontracted the Services to a Third Party which has supplied its services for a price expressed in a currency other than South African Rands, but

d. not more than once in a 12 month period.

14.9 If the Client and Dimension Data fail to agree on the varied Service Charges within 30 days of Dimension Data's notice, either Party may terminate this Agreement by giving 30 days' written notice to the other Party.

Failure to Pay

14.10 If the Client fails to pay any amounts payable to Dimension Data by the due date, Dimension Data may, on 7 (seven) days' written notice, suspend supply of all or any part of the Service until the Client pays all overdue amounts.

Special Charges

14.11 If access to or replacement of a Configuration Item by Dimension Data requires specialised equipment and/or additional resources to comply with legal or occupational health and safety requirements, the Client will incur an Additional Charge.

14.12 Out of scope services performed at a Client Site will attract an Additional Charge.

15. Taxes

15.1 The Service Charges are exclusive of taxes, duties and charges imposed or levied in South Africa in connection with the supply of the Services, and VAT. The Client is liable for any new or altered taxes, duties or charges imposed after the Service Commencement Date in respect of the supply of the Services.

16. Insurance

16.1 During the Term, Dimension Data must:

a. comply with all workers' compensation or similar legislation in respect of its employees and shall obtain and maintain all insurances under and pay all amounts required by that legislation;

b. take out and maintain at its own expense adequate, reasonable insurance cover with a reputable insurer, in respect of Dimension Data's risks under this Agreement; and

c. upon request from the Client provide evidence of each insurance specified in this clause 16.

17. Warranties

17.1 Dimension Data warrants that it will provide the Services in a proper and professional manner and will ensure that the Services are performed by personnel who are suitably qualified to perform the Services.

17.2 The Client warrants that it has the appropriate licenses, rights and/or title to the Configuration Items that are the subject of this Agreement.

17.3 Each Party warrants that:

a. it has the full capacity and authority to enter into this Agreement; and

b. it has the authority to grant any rights, licences and authorisations to be granted to the other Party, and provide any permits or consents, under this Agreement.

17.4 Other than as stated in this clause 17, Dimension Data disclaims all representations and warranties (whether express, implied, arising under statute or otherwise) with respect to the Services provided under this Agreement. This disclaimer includes any express or implied warranties of merchantability and fitness for a particular purpose and non-infringement of title or any Third Party rights, to the extent permitted by Law.

17.5 This clause 17 will survive termination or expiry of this Agreement.

18. Record of Entitlements

18.1 The Record of Entitlements will be subject to change on an ongoing basis as Configuration Items are changed, added and removed in accordance with Dimension Data processes.

18.2 At any point in time the Configuration Items under management will only be as specified in the Dimension Data Management System.

18.3 A baseline list of Configuration Items is specified in the Record of Entitlements. Amendments to this list will be captured and will undergo change control as part of *Service Asset and Configuration Management*.

18.4 Dimension Data will provide an amended Record of Entitlements to Client, if requested.

19. MACD Service Units

19.1 The monthly Service Charges includes MACD Service Units for the term of this Agreement to support Service Requests as defined in in *Part A. Agreement Details*. If Client exhausts the number of service units included in the pricing, Client may purchase additional Service Units.

19.2 With respect to the subsequent purchase of MACD Service Units, Client shall be obliged to purchase a minimum number of 1 MACD bundle (50 Service Units).

19.3 No credit will be provided if there are remaining unused MACD Service Units at the end of the Term.

20. End-of-Life

20.1 If Dimension Data is, in its reasonable opinion, unable to continue to effectively provide the Service for an End-of-Life Configuration Item, Dimension Data may, by giving the Client at least 90 days' prior written notice, remove the End-of-Life Configuration Item from the Record of Entitlement. Upon removal, Dimension Data must make a pro rata adjustment of the Service Charges.

21. Subcontractors

21.1 Dimension Data may subcontract parts of the Services to such persons as it, in its discretion, considers necessary to enable it to fulfil its obligations under this Agreement.

22. Confidentiality

22.1 The Receiving Party acknowledges that the Confidential Information is confidential to the Disclosing Party and is not in the public domain.

22.2 The Receiving Party agrees to:

a. protect the Confidential Information and not reveal or disclose it to any other Party;

b. only use the Disclosing Party's Confidential Information for the performance of its obligations and responsibilities under this Agreement;

c. only disclose the Confidential Information to its personnel on a need-to-know basis; and

d. obtain promises of confidentiality from those personnel who are granted access to the Confidential Information.

22.3 These confidentiality obligations will remain valid for a period of 5 (five) years after the expiry or termination of this Agreement.

22.4 These obligations do not apply to any Confidential Information that:

a. was lawfully in the public domain at the time of disclosure or lawfully becomes available to the general public afterwards;

b. was lawfully known by the Receiving Party at the time it was received;

c. was independently developed by the Receiving Party before the time it was received;

d. was lawfully given to the Receiving Party by a Third Party; or

e. was disclosed in order to comply with a court order or other legal duty, provided that the Receiving Party must only disclose the minimum Confidential Information:

i. required to comply with the court order or other legal duty; and

ii. after having provided as much notice to the other Party as is reasonably practical in the circumstances.

22.5 Each Party must use the same degree of care that it uses to protect its own Confidential Information of a similar nature and value, but in no event less than a reasonable standard of care.

22.6 In the event of a breach by the Receiving Party of any confidentiality obligation, the Receiving Party acknowledges that damages may be inadequate compensation and, subject to the court's discretion, the Disclosing Party may restrain, by an injunction or similar remedy, any conduct or threatened conduct which is or will constitute such a breach.

23. Data Privacy

23.1 In the performance of this Agreement, Client may be required to transfer to Dimension Data Personal Information relating to its staff, directors and officers, agents, subcontractors, independent contractors or other individuals.

23.2 To the extent that any Personal Information is transferred to Dimension Data by Client, Dimension Data shall be allowed to Process Client's Personal Information to perform the required Services. Such Processing shall adhere to the applicable data privacy legislation in the jurisdiction where the Processing occurs. In all circumstances Client will be deemed to be the Data Controller and Dimension Data the Data Processor. Client warrants that the transfer of Client's Personal Information to Dimension Data as well as the Processing of such Client's Personal Information by the latter shall comply with all applicable Laws and regulations on protection of Personal Information.

23.3 To the extent that the Processing of Client's Personal Information by Dimension Data is conducted in accordance with Client's instructions or can be considered as customary usage for the performance of Services, Client shall defend and indemnify Dimension Data from and against any and all claims, liabilities, losses and reasonable expenses incurred by or asserted against Dimension Data in connection with any Third Party claim related to the Processing of Client's Personal Information.

24. Anti-Bribery and Corruption

24.1 Each Party shall comply with the Anti-Bribery Laws including:

a. ensuring that it has in place adequate procedures to prevent bribery;

b. ensuring compliance with the Anti-Bribery Laws;

c. using all reasonable endeavours to ensure that it complies with the other Party's applicable policies relating to prevention of bribery and corruption (as notified to the other Party and as may be updated from time to time); and

d. using all reasonable endeavours to procure that all of that Party's employees, agents, subcontractors and Affiliates involved in performing the Services or with this Agreement so comply.

24.2 Without limitation to the above, neither Party shall make or receive any bribe as defined in the Anti-Bribery Laws, or other improper payment, or allow any such to be made or received on its behalf, and will implement and maintain adequate procedures to ensure that such bribes or payments are not made or received directly or indirectly on its behalf.

25. Intellectual Property Rights – Property Ownership and Licensing

25.1 All Dimension Data Intellectual Property Rights including but not limited to such rights in the Dimension Data Material shall remain the sole and exclusive property of Dimension Data. To the extent it may become necessary do so, Client agrees to execute all documents which Dimension Data may reasonably require to secure and maintain the Intellectual Property Rights in the Dimension Data Material.

25.2 All Intellectual Property Rights in Client Material shall remain the sole and exclusive property of Client.

25.3 Solely for the Term of this Agreement, each Party hereby grants to the other a worldwide, non-exclusive, and non-transferable licence to use the Dimension Data Material or Client

Material (whichever applicable), and only to the extent necessary for Dimension Data to provide, and Client to use, the Services.

25.4 Client shall not, under any circumstances, copy, modify, decompile, reverse assemble, disassemble or make any adaptation or derivative of, sell, resell, transfer, license, sub-license or distribute the Dimension Data Material.

26. Limitations on Liability

26.1 Other than in respect of its liability for death, personal injury, damage to tangible property, or claims for breach of Third Party Intellectual Property Rights, Dimension Data's aggregate liability, whether arising from breach of agreement, negligence or any other tort, breach of warranty under and indemnity or statute, in equity or otherwise is limited to an amount equal to the annual Service Charges paid by Client at the date such liability is proven to have arisen.

26.2 If Dimension Data admits a liability to Client for a claim for a breach of this Agreement and Client has elected not to, (or has no right to) terminate this Agreement on the grounds of the breach, Dimension Data may, at its option, elect to apply the whole or part of any amount agreed to be paid to Client as the result of such breach as a credit to future Service Charges payable by Client.

26.3 Dimension Data has no liability to Client for any incidental, indirect, special or consequential loss or damage, or for loss of or corruption of data, loss of use, revenues, profits, goodwill, bargain, opportunities or anticipated savings, whether arising from breach of agreement, negligence or any other tort, in equity or under an indemnity, warranty or otherwise, whether or not Dimension Data was aware of the possibility of such loss or damage.

26.4 To the fullest extent permitted by Law, the Parties agree to exclude all express or implied warranties, representations, statements, terms and conditions relating to Dimension Data or the provision of the Services under these terms, not expressly set out in these terms, are excluded from the agreement between the Parties.

26.5 Dimension Data will not be liable for any failure or delay in providing the Services where such failure or delay is the direct or indirect result of any action by or the failure of Client to comply with this Agreement.

27. Soliciting Employees or Contractors

27.1 During the term of this Agreement and for 12 (twelve) months after termination by either Party of this Agreement, a Party must not employ or solicit for employment any person who is an employee of or contractor to the other Party who was involved during the most recent 6 (six) month period of this Agreement in the matters covered by this Agreement.

27.2 This clause 27 does not apply where:

a. a person responds to an advertisement for employment by a Party; or

b. the employment is agreed to by the Parties.

27.3 Each Party acknowledges that the restriction specified in this clause 27 is in the circumstances reasonable and necessary to protect each Party’s legitimate interests.

28. Dispute Resolution

Application of Procedure

28.1 Each of the Parties shall use their reasonable endeavours to co-operatively resolve a dispute.

Discussions Between the Parties

28.2 If a dispute arises, the dispute shall be referred to Dimension Data's project manager and Client's representative for resolution.

Referral to a Panel/Executive Panel

28.3 If the dispute is not resolved by Dimension Data's project manager and the Client liaison officer within 5 (five) Business Days of such a referral in accordance with clause28.2, the dispute shall be referred to a panel **("Panel")** for resolution. Each Party shall nominate a representative for the Panel within 5 (five) Business Days of the referral to the Panel in accordance with this clause 28.3.

28.4 If the dispute is not resolved by the Panel within 10 Business Days of such referral, the Panel shall within 3 (three) Business Days refer the dispute for resolution to a Panel comprising the chief executive officer of each Party (or his or her nominee) and the members of the Panel **("Executive Panel").**

28.5 If the dispute is not resolved by the Executive Panel within 10 Business Days of such referral, clause 29 shall apply.

Procedure

28.6 The Panel and the Executive Panel shall determine their own procedures for the resolution of the dispute.

28.7 Decisions of the Panel or the Executive Panel may only be made by unanimous agreement of the members of the Panel or the Executive Panel, as the case may be.

28.8 Any decision of the Panel or the Executive Panel shall be binding on the Parties.

Condition Precedent to Litigation

28.9 Neither Party shall commence legal proceedings unless the Parties have undertaken the process set out in clauses 28.2, 28.3 and 28.4, and those processes have failed to resolve the dispute.

Performance of Obligations Pending Resolution of Dispute

28.10 Prior to the resolution of a dispute, the Parties shall continue to perform their respective obligations to the extent that those obligations are not the subject matter of the dispute.

28.11 Nothing in this clause 28 shall prevent a Party from choosing to perform an obligation which is the subject matter of the dispute.

Injunctive Relief

28.12 Nothing in this clause 28 prevents either Party from seeking urgent injunctive relief against the other Party at any time.

29. Arbitration

29.1 All disputes arising out of or in connection with this Agreement shall be finally settled by arbitration in accordance with the Arbitration Act 42 of 1965 by one arbitrator agreed upon by the Parties. If such appointment is not agreed to within 7 (seven) days after receipt of written notice from a Party requesting such agreement, either Party may request that the

President of the Law Society of the Northern Provinces (or any successor to such society) make the necessary appointment.

29.2 The seat of the arbitration shall be South Africa.

29.3 The language of the arbitration shall be English.

29.4 The arbitration, including documents and evidence produced in the arbitration, and the content of any award shall be confidential to the Parties.

29.5 The Parties agree that an arbitral tribunal constituted under this clause 29 may, unless consolidation would prejudice the rights of any Party, consolidate an arbitration commenced hereunder with arbitration under any other contract if the arbitration proceedings raise common questions of law or fact or if it is otherwise convenient to do so. If two or more arbitral tribunals under these agreements issue consolidation orders, the order issued first shall prevail.

29.6 This clause 29 shall survive termination of this Agreement.

30. Suspension

30.1 Without prejudice to any other rights or remedies it might have available at Law, or under this Agreement, Dimension Data may suspend the provision of Services:

a. where Client commits a material breach of this Agreement (and for so long as that breach continues);

b. where an undisputed Service Charge owing remains unpaid at the expiry of 30 (thirty) days after the due date for payment;

c. in the event of an emergency with respect to the Dimension Data system or network, or if Dimension Data reasonably believes that the integrity and security of the Dimension Data system or network is at risk or has been compromised or to maintain, repair or enhance the performance of the Dimension Data system or network; and/or

d. where it is required to do so by any applicable Law.

30.2 All applicable Service Charges in relation to the Services will continue to apply during any period of suspension in terms of clauses 30.1a and/or .

30.3 Dimension Data will not be liable for any loss or inconvenience suffered by Client as a result of any suspension in terms of this clause 30.

31. General Conditions

Other Terms

31.1 Terms or conditions attached to or forming a part of a purchase order that Client issues do not form part of this Agreement.

Governing Law

31.2 This Agreement is governed by the laws of the Republic of South Africa.

Prior Agreements

31.3 This Agreement supersedes all prior agreements, arrangements and undertakings between the Parties and constitutes the entire agreement between the Parties relating to its subject matter.

Variations

31.4 No variation of this Agreement, including this clause, is binding upon the Parties unless made in writing signed by an authorised representative of each of the Parties, unless provided otherwise in this Agreement. Dimension Data's written acceptance of a written request (including a request made by e-mail) by Client for a variation to the Record of Entitlements is binding on both Parties. Following an agreed variation, Dimension Data must issue a revised Record of Entitlements.

Notices

31.5 Notices to or by a Party delivered in person are deemed to be given by the sender and received by the addressee when delivered to the addressee: if by post, 3 (three) Business Days from and including the date of postage; or if by facsimile, when successfully transmitted to the addressee provided that if transmission is on a day which is not a Business Day or is after 5.00 PM (addressee's time), on the Next Business Day.

Illegality

31.6 Any provision or the application of any provision of this Agreement which is void, illegal or unenforceable in any jurisdiction does not affect the validity, legality or enforceability of that provision in any other jurisdiction or of the remaining provisions in that or any other jurisdiction.

Waiver

31.7 A waiver of a breach of this Agreement or of any right, power, authority, discretion or remedy arising upon a breach of or default under this Agreement must be in writing and signed by the Party granting the waiver.

Assignment

31.8 A Party may only assign this Agreement and any rights under this Agreement with the prior written consent of the other Party, provided that Dimension Data may assign any of its rights or obligations under this Agreement to any Dimension Data affiliate, without the prior written consent of Client.

Dimension Data Management System

31.9 Due to changes in technology and Dimension Data's desire to maintain the highest possible quality of the Services, it may be necessary to make adjustments or add enhancements to the Dimension Data Management System during the Term. Dimension Data will provide advance notice of any such changes, if possible. If the Scope of Service is necessarily improved or extended as a result of the enhancements, they will be offered to Client for the remainder of the then current Term at no additional cost, provided that Dimension Data will expect that no claim is made for a reduction in the Service Charges for minor reductions in scope as a result of the enhancements.

Force Majeure and Excused Performance

31.10 Neither Party is liable to the other for the consequences of any delays or failures of its performance which are caused by a Force Majeure Event.

31.11 If any *Force Majeure* Event occurs in relation to either Party that affects or may affect the performance of any of its obligations under this Agreement, it shall forthwith notify the other Party as to the nature and extent of the circumstances in question. Neither Party shall be deemed to be in breach of this Agreement, or shall otherwise be liable to the other, by reason of any delay in performance, or the non-performance of any of its

obligations under this Agreement to the extent that the delay or non-performance of that obligation is due to any *Force Majeure Event* of which it has notified the other Party and the time for performance shall be extended accordingly.

31.12 If the performance by either Party of any of its obligations under this Agreement is prevented or delayed by a *Force Majeure Event* for a continuous period in excess of 30 (thirty) days, the other Party shall be entitled to terminate this Agreement by giving written notice to the Party so affected, whereupon all money due up to the point of termination under this Agreement shall be paid immediately, and in particular Client shall pay to Dimension Data all arrears of payment.

31.13 Dimension Data will not be liable for any failure or delay in providing the Services, or any non-achievement of Service Level Targets, to the extent such failure or delay or non-achievement is the direct or indirect result of any act or omission by Client or the failure of Client to comply with any of its responsibilities and obligations under this Agreement.

31.14 Dimension Data will not be liable for Service Level Target failures resulting from:

a. power outages;

b. a failure of Third Party supplied equipment and/or services; and/or maintenance of such equipment or services;

c. errors caused by Client or its end users; and

d. a Force Majeure Event.

Part D. Transition

32. Transition

Client Transition

32.1 Dimension Data will perform a Client Transition as part of the Services, utilising Dimension Data methodologies and templates.

32.2 If not conducted prior to the acceptance of this Agreement, a discovery of Client's environment may be conducted by Dimension Data in consultation with Client to determine whether Dimension Data is capable of providing the Service and whether all requirements in respect of providing the Service have been met.

32.3 All Transition activities will be documented by Dimension Data in consultation with Client. These include but are not limited to:

a. Service enablement or activation activities;

b. technical documentation;

c. Client and internal training;

d. call flow processes;

e. reporting requirements; and

f. operations RACI.

32.4 Transition activities only covers activities conducted during a Business Day. Additional charges may apply if work is required to be performed outside of a Business Day.

32.5 Any travel costs incurred during Transition will be charged to the Client separately and in addition to the Charges.

32.6 The Configuration Items set out in the Record of Entitlements will be validated during Transition.

32.7 If the quantity of the validated Configuration Items differs from the quantity of Configuration Items listed in the Record of Entitlement, a variation may be made to the Service Charges.

32.8 Responsibilities in respect of all activities between the Parties will be set down in writing in advance in a Transition RACI.

32.9 Risks and issues will be identified, prioritised and assigned.

32.10 Out of scope items will be documented.

Transition Schedule

32.11 The Parties will, where applicable, prepare and document a Transition schedule.

32.12 The Parties shall complete the Transition activities and milestones in accordance with the Transition schedule.

32.13 The Transition schedule will be reviewed and approved during the planning phase of Transition by all stakeholders.

Transition Governance

32.14 Meetings and meeting structure is to be agreed in the Client kickoff meeting.

32.15 An escalation path matrix or diagram will be shared with the transition scope document.

Transition Exclusions

32.16 Migration and integration services are not included in the monthly fees or as part of this Agreement. If Client requires Dimension Data to carry out migration or integration services,

such shall be treated and charged for as a separate Consulting and Professional Services engagement.

Transition Re-Initiation

32.17 Client Transition will be re-initiated in accordance with the relevant scope of work (or similar) document if Client has purchased MSS Threat Detection (Standard or Enhanced) or MSS Enterprise Security Monitoring (Standard or Enhanced), Transition may be re-initiated if:

a. materially modified Source feeds constitute a coding change to the classifier in use; and

b. any of the operating systems or applications resident on any of the originally contracted devices are materially altered.

33. Exit Assistance

33.1 Dimension Data shall, during the exit assistance period provide exit assistance services. The exit assistance period starts on a date mutually agreed between Client and Dimension Data.

33.2 Dimension Data shall be paid all applicable Service Charges (as set out in *Part A. Agreement Details*) rendered during the exit assistance period.

33.3 During the exit assistance period Dimension Data will continue to perform its obligations under this Agreement.

33.4 Dimension Data agrees to provide reasonable assistance, acting in a manner consistent with Good Industry Practice, for the Transition of Client data and/or domain names following the termination of this Agreement provided that the termination occurred for reasons other than the unresolved material breach of the Client. Such assistance shall be treated and charged for as a separate Consulting and Professional Services engagement.

33.5 Client agrees to use commercially reasonable efforts during the exit assistance period to expeditiously terminate the Services provided by Dimension Data. Throughout the exit assistance period, Dimension Data agrees it will maintain the Service Level Targets specified in respect of the Services.

Part E. Common Service Features

34. General Obligations

34.1 Dimension Data must, for the purpose of supplying the Services, provide the Service Packages selected by the Client and specified in the Record of Entitlement.

34.2 The Service Features set out in the table below are described in further detail in clauses 35 to 42 inclusive.

34.3 Table of Service Features:

Page Ref.	Service Features
35	**Security Incident Management**
	Call Management
	Security Incident Resolution
	Security Incident Reporting
36	**Availability Management**
	Availability Event Monitoring and Reporting
	Availability Improvement Recommendation
	Availability Planning
37	**Event Management**
	Event Handling
	Event Optimisation
38	**Capacity and Performance Management**
	Capacity Event Monitoring and Reporting
	Capacity Improvement Recommendation
	Capacity Planning
	Performance Needs Analysis
	Performance Policy Definition
	Performance Monitoring and Reporting
	Performance Improvement Recommendations
39	**Service Asset and Configuration Management**
	Configuration Item Identification and Recording
	Vendor Update Notification
	Configuration Item Control and Updates
	Configuration Item Data
	Documentation Maintenance
	Configuration Item Status Reporting
40	**Change Management**
	Change Request Management
	Change Impact Analysis

Page Ref.	Service Features
	Change Planning
	Change Implementation
	Change Reporting
41	**Request Fulfilment**
	Service Request Management
	Standard Changes
	Request for Information Fulfilment
	Service Request Reporting
42	**Service Level Management**
	Service Level Monitoring and Reporting
	Service Management Review Meeting

35. Security Incident Management

Call Management

Dimension Data's obligations

35.1 Dimension Data must raise a Security Incident Record as a result of:

a. Client logging a Security Incident with Dimension Data through the Service Desk; or

b. Client logging a Security Incident with Dimension Data via the Service Portal; or

c. detection of an Event on monitored Configuration Items.

35.2 Following the creation of a Security Incident Record, Dimension Data will respond to Client to confirm the initial Security Incident classification and prioritisation.

The Client's obligations

35.3 The Client must:

a. raise Priority 1 and 2 Security Incidents with the Service Desk by telephone only; and

b. provide Dimension Data with Client contacts authorised to log Security Incidents, and notify Dimension Data of any changes to these contacts.

35.4 Client may request the escalation of a Security Incident to a higher Priority by contacting an escalation manager through the Service Desk and quoting the reference number.

35.5 Dimension Data may downgrade an escalated Security Incident if it is being managed to a scheduled timeframe, or resolution has been provided to Client and is in the process of being tested.

35.6 Where Client initiated the escalation, Dimension Data will obtain Client's approval prior to downgrading.

Security Incident Resolution

Dimension Data's obligations

35.7 Once the Security Incident is resolved, Dimension Data must:

a. close the Security Incident Record; and

b. notify Client of resolution and closure of the Security Incident Record.

35.8 Where a Security Incident is caused by Client making changes to Configuration Items, Client may incur an Additional Charge.

Security Incident Reporting

Dimension Data's obligations

35.9 Dimension Data must provide Client with Security Incident management reporting information, including:

a. statistical information in respect of Security Incident management; and

b. Security Incident management Service Level Target achievement.

36. Availability Management

Availability Event Monitoring and Reporting

Dimension Data's obligations

36.1 Dimension Data must:

a. monitor for the availability of Configuration Items within the agreed Service Calendar;

b. detect availability-related Events (where the monitoring tools are supported and managed by Dimension Data);

c. where required, initiate the Security Incident management process, as described in clause 35; and

d. notify Client that the Security Incident management process has been initiated.

36.2 Dimension Data will provide Client with availability data, including:

a. statistical information in respect of availability Events; and

b. availability management Service Level Target achievements, where applicable.

Availability Improvement Recommendation

36.3 Clauses 36.4 and 36.5 only apply if the Client has purchased the Additional Management Option Service Package.

Dimension Data's obligations

36.4 Dimension Data must periodically, analyse the available data to assess where a Configuration Item's availability could be improved.

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

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

b. where possible, the estimated cost of the remediation or recommendation by Dimension Data.

Availability Planning

36.6 Clause 36.7 only applies if the Client has purchased the *Additional Management Option* Service Package.

Dimension Data's obligations

36.7 Dimension Data must periodically, as agreed with Client:

a. work with Client to understand future availability requirements;

b. analyse the available data to identify any expected availability concerns in the context of Client requirements;

c. assess possible remedial actions and recommendations for expected availability concerns;

d. document the results in an initial Availability Plan created after the first 3 (three) months, and updated every 3 (three) months thereafter; and

e. provide Client with the Availability Plan for review and sign-off.

37. Event Management

Event Handling

Dimension Data's obligations

37.1 Dimension Data must:

a. monitor for Events within the agreed Service Calendar;

b. assess Events against predefined rules;

c. where possible, resolve Events automatically; or

d. route Events accordingly to the relevant process for investigation and resolution.

Event Optimisation

Dimension Data's obligations

37.2 The Client must, periodically:

a. identify opportunities to optimise Event handling; and

b. where possible, add new automation rules to the Dimension Data Management System.

38. Capacity and Performance Management

38.1 This clause 38 only applies if the Client has purchased the *Additional Management Option* Service Package.

Capacity Needs Analysis

Dimension Data's obligations

38.2 Dimension Data must:

a. analyse Client's capacity needs, based on information requested by Dimension Data and provided by the Client; and

b. document and make available the results of the capacity needs analysis.

Capacity Event Monitoring and Reporting

Dimension Data's obligations

38.3 Dimension Data must provide Client with capacity data, including:

a. statistical information in respect of capacity Events; and

b. capacity management Service Level Target achievement, where applicable.

The Client's obligations

38.4 The Client must:

a. monitor capacity utilisation of Configuration Items within the agreed Service Calendar;

b. detect capacity-related Events;

c. where required, initiate the Security Incident management process, as described in clause 35; and

d. notify Client that the Security Incident management process has been initiated.

Capacity Improvement Recommendation

Dimension Data's obligations

38.5 Dimension Data must periodically analyse the available data to determine where a Configuration Item's capacity could be improved.

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

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

b. where possible, the estimated cost of the remediation or recommendation by Dimension Data.

Capacity Planning

Dimension Data's obligations

38.7 Dimension Data must, periodically, as agreed with Client:

a. work with Client to understand its future capacity requirements;

b. analyse the available data to identify any expected capacity concerns in the context of Client's requirements;

c. assess possible remedial actions and recommendations for expected capacity concerns;

d. document the results in an initial Capacity Plan created after the first 3 (three) months, and updated every 3 (three) months thereafter; and

e. provide Client with the Capacity Plan for review and sign-off.

Performance Needs Analysis

Dimension Data's obligations

38.8 Dimension Data must:

a. analyse Client's performance needs, based on information requested by Dimension Data and provided by Client for an Additional Charge on a time and material basis; and

b. document and make available the results of the performance needs analysis.

Performance Policy Definition

Dimension Data's obligations

38.9 Dimension Data must, in agreement with Client, define acceptable system performance policies for the Services, based on:

a. a performance needs analysis;

b. feasibility of Client's performance requirements; and

c. Client's established performance baseline.

Performance Monitoring and Reporting

Dimension Data's obligations

38.10 Dimension Data must, in accordance with the performance policy:

a. monitor performance within the agreed Service Calendar;

b. detect performance-related Events;

c. where required, initiate the Security Incident management process, as described in clause 35; and

d. notify Client that the Security Incident management process has been initiated.

38.11 Dimension Data must provide Client with performance reporting data, including:

a. statistical information in respect of performance Events; and

b. performance management Service Level Target achievement, where applicable.

Performance Improvement Recommendations

Dimension Data's obligations

38.12 Dimension Data must periodically analyse the available data to determine where performance could be improved.

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

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

b. where possible, the estimated cost of the remediation or recommendation by Dimension Data.

39. Service Asset and Configuration Management

Configuration Item Identification and Recording

Dimension Data's obligations

39.1 Dimension Data must:

a. record pre-defined Configuration Items, as set out in the Record of Entitlements; and

b. provide Client with access to this information.

Vendor Update Notification

Dimension Data's obligations

39.2 Dimension Data must provide the Client with relevant vendor notification information, including:

a. patches;

b. end-of-X milestones;

c. minor feature releases; and

d. security vulnerabilities.

39.3 Dimension Data can only notify Client in terms of clause 39.2 in the event that it receives the notification from the relevant Manufacturer. Accordingly, and for the avoidance of doubt, where the Manufacturer does not provide notifications in respect of a Configuration Item (for example that the Configuration Item has reached End-of-Life), Dimension Data will not be liable for performance of this Service Feature.

Configuration Item Control and Updates

Dimension Data's obligations

39.4 Where, in Dimension Data's performance of the Services, a Configuration Item's Attributes are altered, Dimension Data will update the Attributes accordingly.

39.5 Where Client makes changes to a Configuration Item's Attribute, Client must promptly notify Dimension Data by raising a Service Request.

Configuration Item Data

Dimension Data's obligations

39.6 Dimension Data must:

a. use Dimension Data and/or Manufacturer data sets to enrich the Client-provided Configuration Item data with additional, applicable information; and

b. have exclusive write access to all Configuration Items covered by the Service.

39.7 In addition to any Client responsibilities set out in this Agreement, Client must, no less than 5 (five) Business Days prior to the agreed scheduled discovery activity:

a. notify its operational and security teams, as applicable, and implement appropriate change controls to avoid 'false positive' security alerts; and

b. provide Dimension Data with a management IP address that is included in SNMP ACLs and all firewall rules.

Documentation Maintenance

Dimension Data's obligations

39.8 Dimension Data must create and maintain documentation relating to the Configuration Items under the Services, which may include:

a. system manuals;

b. network diagrams;

c. wide-area network carrier topology;

d. network and engineering diagrams for specific Client Sites;

e. contact information for Client Sites; and

f. configuration standards and guidelines.

Configuration Item Status Reporting

Dimension Data's obligations

39.9 Dimension Data must provide Client with service asset and configuration management data through the Service Portal, including:

a. statistical information in respect of Configuration Items; and

b. service asset and configuration management Service Level Target achievement, where applicable.

40. Change Management

Change Request Management

Dimension Data's obligations

40.1 Dimension Data must raise a Change Request record as a result of:

a. Client logging a Change Request with Dimension Data through the Service Desk;

b. Client logging a Change Request with Dimension Data via the Service Portal; or

c. by Dimension Data, as part of the performance of its obligations under a Service Feature.

40.2 Following the creation of a Change Request record, Dimension Data will respond to Client to confirm the initial Change Request classification.

40.3 Dimension Data will manage the lifecycle of a Change Request in accordance with the Change Request classification.

Change Impact Analysis

Dimension Data's obligations

40.4 Based on the information available, Dimension Data must assess and determine the impact of a Change Request on:

a. the Configuration Items; and

b. the forward schedule of changes, as advised by Client.

40.5 Dimension Data will make the results of the change impact analysis available to Client.

Change Planning

Dimension Data's obligations

40.6 Dimension Data must produce a Change Plan, with input from Client, for Change Requests, that includes:

a. where possible, a test plan for testing the change prior to roll-out;

b. tasks for the implementation of the change;

c. determination of the number and availability of Dimension Data and Client representatives required to implement the change;

d. identification of any additional ongoing resources required once the change is implemented;

e. a plan for the roll-back of a failed or failing change;

f. calculation of the time required to implement the change; and

g. the number of MACD Service Units required to implement the change.

40.7 Dimension Data will submit the Change Plan to Client for approval and for submission to the Client's Change Advisory Board, if applicable.

40.8 Dimension Data will participate in Client's Change Advisory Board meetings as required.

Change Implementation

Dimension Data's obligations

40.9 Dimension Data must, upon receipt of approval from Client to proceed, implement the Change Request according to the approved Change Plan.

40.10 On completion, the relevant number of MACD Service Units for Service Requests will be deducted in accordance with the Change Plan or as agreed with Client:

a. on a time and materials basis at an Additional Charge;

b. through remote fulfilment of Service Requests, where applicable, and as per the process set out in clause 41; and/or

c. through a formal Consulting and Professional Services engagement, the scope and pricing of which will be agreed with Client and set out in a separate Scope of Service.

40.11 Dimension Data will implement changes to Configuration Items in alignment with the agreed change management process, as notified by Client and agreed to by Dimension Data, to the extent practicable.

Change Reporting

Dimension Data's obligations

40.12 Dimension Data must provide Client with change management reporting information, including:

a. statistical information in respect of change management; and

b. change management Service Level Target achievement, where applicable.

41. Request Fulfilment

Service Request Management

Dimension Data's obligations

41.1 Dimension Data must raise a Service Request as a result of:

a. Client logging a Service Request with Dimension Data through the Service Desk; or

b. the Client logging a Service Request with Dimension Data via the Service Portal.

41.2 Following the creation of a Service Request record, Dimension Data will respond to Client to confirm the initial Service Request classification and prioritisation.

41.3 Client may request the escalation of a Service Request to a higher Priority by contacting an escalation manager through the Service Desk and quoting the reference number.

41.4 Dimension Data may downgrade an escalated Service Request if it is being managed to a scheduled timeframe, or where a resolution has been provided to Client and is in the process of being tested.

41.5 Where Client initiated the escalation, Dimension Data will obtain Client's approval prior to downgrading.

41.6 Client must log Priority Service Requests with the Service Desk by telephone or via the Service Portal with a follow up telephone call.

Standard Changes

41.7 A Service Request is a Standard Change, which:

a. is pre-approved by Client;

b. relates directly to a Configuration Item;

c. can be performed remotely using the site-to-site connection;

d. is executable by a vendor-certified engineer;

e. requires no scoping or project management for its completion;

f. should not as a single task take more than 2 (two) hours to perform;

g. when performed as part of a set of requested tasks (i.e. repeating the same single instance or similar tasks in multiple Client Sites or for multiple Configuration Items) does not take more than 4 (four) hours to perform; and

h. has a set of procedures/work instructions available to complete.

41.8 Where a Service Request is raised:

a. the Service Request is considered pre-approved by Client;

b. Dimension Data will schedule the implementation of the Service Request as agreed with Client; and

c. should the Service Request as a single task take more than 2 (two) hours to perform or include multiple tasks that exceed 4 (four) hours of effort, Dimension Data will perform the work, as agreed with Client:

i. on a time and materials basis at an Additional Charge; and/or

ii. through a formal Consulting and Professional Services engagement, the scope and pricing of which will be set out in a separate Scope of Service.

41.9 Dimension Data will fulfil the Service Request through utilising a MACD Service Unit system, whereby MACD Service Units are purchased in advance by Client and deducted on execution.

41.10 MACD Service Units will expire on the expiration of the Services and will not be refunded to Client.

41.11 For the avoidance of doubt, Client will remain responsible for the mitigation of any risks associated with the implementation of the Service Request and ensure changes are internally approved and communicated.

Request for Information Fulfilment

41.12 Where Client raises a Service Request for information in respect of a procured service product Dimension Data will use commercially reasonable efforts to collate the required information and supply it to Client at no Additional Charge.

41.13 Where Client raises a Service Request for information which is neither in respect of a procured Service, nor executable with commercially reasonable efforts, Dimension Data reserves the right to fulfil the request for information on a time and materials basis at an Additional Charge.

Service Request Reporting

Dimension Data's obligations

41.14 Dimension Data must provide Client with Service Request reporting information, including:

a. statistical information in respect of Service Requests;

b. information in respect of MACD Service Unit usage; and

c. Service Request Service Level Target achievement, where applicable.

42. Service Level Management

Service Level Monitoring and Reporting

Dimension Data's obligations

42.1 Dimension Data must monitor its performance against the Service Level Targets agreed with Client, and will make monthly Service management information available to Client.

42.2 The service level information does not include reporting on any Service Levels Targets agreed between Client and a Third Party.

42.3 Dimension Data may, on written request by Client, agree to produce customised or additional reporting at an Additional Charge.

Service Management Review Meeting

Dimension Data's obligations

42.4 Dimension Data must:

a. schedule a regular service management review meeting with Client, as agreed between the Parties; and

b. compile and distribute a copy of the meeting notes to Client within a reasonable timeframe.

42.5 Items to be discussed at the meeting may include any previously agreed actions and associated timeframes agreed going forward.

42.6 The Parties must make suitably skilled representatives available to attend a service management review meeting.

42.7 Should Client require Dimension Data to attend a service management review meeting at Client Site more than 100 kilometres from a Dimension Data office, Client shall notify Dimension Data no less than 10 Business Days prior to the review meeting and reimburse Dimension Data for associated travel expenses.

Part F. Service Level Targets

43. Service Level Targets

43.1 Dimension Data will use commercially reasonable endeavours to ensure that the Services are performed to the specified Service Level Targets.

43.2 Dimension Data may, from time to time, issue a notice varying or modifying the terms of the Service Level Targets, where the variation or modification does not reduce the Service Level Target commitment or prejudice Client in any way. Such variation or modification will be effective from the date of notice, unless otherwise set out therein.

43.3 If Dimension Data's ability to perform its obligations are dependent on Client and/or a Third Party contracted to Client to perform certain activities, Dimension Data's Service Level Targets will be suspended until the work is completed.

43.4 The Service Level Targets will apply in respect of the Services as follows:

Security Incident notification

a. Dimension Data will monitor for Events which may impact availability and capacity Attributes, specifically with respect to availability failures which result in Services and capacity thresholds not being met. Should there be an Event which causes such impact, the Event will be categorised by Dimension Data as a Security Incident and Client will be notified within 30 minutes of the Security Incident being logged by Dimension Data.

b. Dimension Data shall meet the Security Incident notification Service Level Target in respect of no less than 95% (ninety-five percent) of all Security Incidents closed in a given calendar month.

Security Incident response time

c. Dimension Data will respond to Security Incidents reported by Client as per the table below.

d. Dimension Data shall meet this Service Level Target in respect of no less than 95% (ninety-five percent) of all Security Incidents closed in a given calendar month.

Priority	Response Time
1 – Critical	30 minutes
2 – High	60 minutes

Security Incident restoration time

a. Dimension Data will restore Security Incidents as per the table below.

b. Dimension Data shall meet this Service Level Target in respect of no less than 95% (ninety-five percent) of all Security Incidents closed in a given calendar month.

Priority	Restore Time
1 – Critical	4 hours
2 – High	8 hours
3 – Medium	24 hours

Request fulfilment response time

a. Dimension Data will respond to requests for information and Standard Changes as per the table below.

b. Dimension Data shall meet this Service Level Target in respect of no less than 95% (ninety five percent) of all defined requests in a given calendar month.

Feature	Action	Response Time
Request for Information	Response	48 hours
Standard Changes	Response	48 hours

Request fulfilment time

a. Dimension Data will fulfil requests for information and Standard Changes as per the table below.

b. Dimension Data shall meet this Service Level Target in respect of no less than 95% (ninety five percent) of all defined requests in a given calendar month.

Feature	Action	Response Time
Request for Information	Fulfilment	48 hours
Standard Changes	Fulfilment	48 hours

Part G. Reporting

44. Service Management Reporting

44.1 The table below specifies all Service management reports, and defines the respective methods of delivery and frequency:

Report Contents	Delivery	Frequency
Operations Summary which includes information on: • Service Level Target achievement • Change management • Configuration and Inventory • Request fulfilment • Problem management • MACD Service Unit consumption	Monthly service review meeting	Monthly

45. Self-Service Reporting

45.1 A standardised set of self-service dashboards and access to data for the Services are available on the Service Portal.

Appendix A. Scope of Service – MSS Threat Detection

1. Definitions and Interpretations

1.1 For the purposes of this Scope of Service, and in addition to the definitions in clause 1 of the Agreement:

"Advanced Analytics" means detection capabilities, including machine learning, statistical modelling, kill-chain modelling, big data, and complex event processing analysis, that are included as part of the Service.

"Event-Driven Threat Hunting" means threat hunting performed by security analysts intended to investigate, validate, and determine the breadth and scope of a detected Event or Security Incident in a Client environment.

"Global Threat Intelligence Centre (GTIC)" means the Dimension Data Security organisation responsible for Security Incident response and forensics, threat research, and vulnerability tracking.

"Global Threat Intelligence Platform (GTIP)" means a threat intelligence gathering and curation platform developed and maintained by Dimension Data.

"Log Transport Agent (LTA)" means the Software responsible for facilitating the transport of Log data between Source devices and the Security Appliance using common Log transport mechanisms (for example, syslog, API, custom Software). Depending on the type of LTA in use, the LTA will reside either on the monitored Source, or on the Security Appliance.

"Notification" means an email to Client communicating the occurrence of a Security Incident.

"Notification Procedures" means documentation of how Clients will be contacted for different service scenarios. Notification Procedures are developed in collaboration with the Client during Transition.

"Security Appliance" means enablement of the Service by physical or virtual collection and forwarding of Logs for analysis.

"Source" means a device (for example, application, OS, database) that generates a Log, Event, report, or evidence used in the operation of the Service.

2. Service Scope

2.1 MSS Threat Detection is available in Standard or Enhanced Service Packages, consisting of the Service Features set out in the table below, and cannot be selected or deselected for a specific Configuration Item.

2.2 The Service Features common to all Managed Security Services listed in the table below are defined in further detail in *Part E. Common Service Features*. The Service Features specific to MSS Threat Detection listed in the table below are defined in further detail in clauses 4 to 10 inclusive.

2.3 Table of Service Features:

MSS Threat Detection Service Features	Service Package	
	Standard	Enhanced
Service-specific Service Features		
Security Appliance	✓	✓
Detection Type	✓	✓
Threat Intelligence	✓	✓

MSS Threat Detection Service Features	Service Package	
	Standard	Enhanced
Security Analyst Interaction		✓
Client Notification	✓	✓
Investigator Log Search Capability		Optional
Portal and Reporting	✓	✓
Common Service Features		
Incident Management	✓	✓
Availability Management	✓	✓
Event Management	✓	✓
Capacity and Performance Management	✓	✓
Service Asset and Configuration Management	✓	✓
Change Management	✓	✓
Request Fulfilment	✓	✓
Service Level Management	✓	✓

3. Service Exclusions

3.1 Dimension Data:

a. will not support altered, damaged, or modified Software, or Software that is not a supported version within the Service; and

b. will only be responsible for management and maintenance of the appliance Software (in both physical and virtual form factors), and the physical form factor if supplied by Dimension Data.

Service-Specific Service Features

4. Security Appliance

4.1 Dimension Data must gather Logs, Events, reports, and evidence data from Client devices and systems, then prepare the data for secure transmission and processing.

5. Detection Type

5.1 Dimension Data must use Advanced Analytics with proprietary machine learning / behavioural modelling to detect threats in Client environment, leveraging a combination of traditional threat detection techniques, for example:

a. correlation;

b. pattern matching; and

c. reputation feeds

5.2 Dimension Data must use threat intelligence to detect sophisticated threats in the Client environment.

5.3 If Client has purchased the *Enhanced* Service Package, Dimension Data must ensure service quality by detecting tuning decisions based on the validity and relevance of Service-generated Events and Security Incidents on a continuous basis.

6. Threat Intelligence

6.1 Dimension Data must use threat intelligence to:

a. analyse internal and external threats that may impact the Client's organisation;

b. enrich the defensive abilities against known threats including malware, malicious devices, known exploits, and advanced persistent threats from a global perspective;

c. deliver Threat Intelligence from the Global Threat Intelligence Centre (GTIC); and

d. provide continuous Threat Intelligence updates driven by investigations of actual Security Incidents.

7. Security Analyst Interaction

7.1 If Client has purchased the *Enhanced* Service Package, Dimension Data must:

a. identify suspicious activities and present all relevant contextual information to a skilled security analyst located in a Security Operations Centre (SOC), who must:

i. engage in Event-Driven Threat Hunting and threat validation activities in Client's in-scope Log monitoring and/or telemetry environment;

ii. validate and assess the malicious nature of a threat and its potential impact;

iii. identify additional information associated with the potential breach;

iv. create a detailed Security Incident Report;

v. initiate Security Incident Notifications in accordance with documented Client Notification Procedures; and

vi. provide a detailed description of the Security Incident combined with scenario-specific actionable response recommendations to significantly assist Client to lower associated risks by reducing the amount of time taken to take informed responsive measures;

b. integrate vendors and collect evidence for selected security technologies including:

i. packet capture data (PCAP);

ii. malware execution reports; and

iii. host recordings; and

c. define selected security technologies in a Technology Solution Guide and make available to Client during Transition.

8. Client Notification

8.1 If Client has purchased the *Standard* Service Package, Dimension Data must ensure Client receives automated Security Incident Report Notifications via email.

8.2 If Client has purchased the *Enhanced* Service Package, Dimension Data must:

a. provide a Security Incident Report based on detailed investigation and Event-Driven Threat Hunting, prepared by a Security Analyst; and

b. notify Client based on Client's selection of Notification options, for example via email or telephone.

9. Investigator Log Search Capability

9.1 If Client has purchased the optional *Investigator Search Log Capability* as part of the Enhanced Service Package, Dimension Data must provide Client with access to an interface to perform historical Log searches.

10. Service Portal and Reporting

10.1 Dimension Data must provide Client with access to the previous ninety (90) days of Event and Security Incidents via the Service Portal.

Service-Specific Obligations

11. General Obligations

11.1 The Client must:

a. procure all maintenance, support, and licensing agreements with Third Party vendors for all non-Dimension Data provided in-scope devices for the term of the Agreement, unless otherwise stated in the purchase order;

b. work with Dimension Data to amend the purchase order accordingly if any devices are not compliant with the configuration guidance, including use of supported versions of Source devices only;

c. work with Third Party vendors to rectify device failure for all non-Dimension Data provided devices and be responsible for all associated expenses;

d. ensure compliance with all relevant data privacy, regulatory, and administrative policies and procedures related to monitoring of user traffic and communications;

e. notify Dimension Data and assist Dimension Data to identify and develop a mutually agreed mitigation plan if Client utilises security technologies that blocks traffic, rotates Logs, or otherwise impedes the ability of the Service to receive Logs from in-scope devices;

f. ensure the physical security of all Security Appliances located at Client Site or hosted at Third Party locations;

g. resolve Client Internet Service Provider (ISP) outages, or issues with Client internal network infrastructure; and

h. work with Dimension Data to amend the scope of work accordingly if:

i. regulatory changes (including, without limitation, changes by a regulatory agency, legislative body, or court of competent jurisdiction) require a modification to the Services described herein; and

ii. Client's environment generates an inordinate number of Logs or Events processed by the Service.

12. Access Requirements

12.1 The Client must:

a. be responsible for selecting Services and ensuring that the Service meets any and all compliance standards (for example, PCI, HIPAA) which apply;

b. assign a main Client Point of Contact (POC) to be available during all scheduled activities;

c. ensure that the assigned Client POC works with Dimension Data to schedule all Service-related activities and communicate with Dimension Data as needed for installation and ongoing tuning and support;

d. complete all reasonably required information for Transition in a timely manner;

e. notify Dimension Data in a timely manner of any changes to Client contacts for Security Incident escalation;

f. maintain Service Portal user list and rights;

g. provide access and connectivity to all Configuration Items, including the ability to receive Source feeds and evidence data including, without limitation, packet capture and stack trace;

h. provide knowledgeable technical staff, and/or Third Party resources, to assist with Hardware and Software implementations, including, without limitation:

i. configuring end-to-end connectivity to ensure the successful transport of all in-scope Log feeds and evidence data;

ii. providing rack space and power for each in-scope Security Appliance (if applicable);

iii. providing an IP address for each Security Appliance to be installed at Client Site;

iv. installing Security Appliances on Client network;

v. installing Log Transport Agents (LTAs) in accordance with the instructions supplied by Dimension Data; and

vi. working with Third Party vendors for support or provide authorisation for Dimension Data to contact Third Party vendors on behalf of Client as appropriate;

i. ensure Source device and LTA configurations comply with the standard setup requirements for the Service which will be made available during Transition; and

j. install, initially configure and enroll all Security Appliances in accordance with the guidance provided during Transition.

12.2 Dimension Data recommends that Client performs full backups of relevant systems prior to the performance of services.

12.3 If Client's configuration cannot or does not comply with configuration guidance, engineering consulting hourly rates will apply to develop a custom solution.

Appendix B. Scope of Service – MSS Enterprise Security Monitoring

1. Definitions and Interpretations

1.1 For the purposes of this Scope of Service, and in addition to the definitions in clause 1 of the Agreement:

"Complex Analysers" means a detection mechanism that requires detailed analysis and development (e.g. Malicious User Analyser – a complex analyser which monitors for repeat failed logins followed by a successful login on the same service from same source IP and user ID).

"Compound Rules" means an enhanced detection type that tests multiple attributes to generate an Event (e.g. if more than 5 failed logins from a specific account occur after business hours, then an Event should be generated).

"Log Transport Agent (LTA)" means the software responsible for facilitating the transport of Log data between Source devices and the Security Appliance using common Log transport mechanisms (for example, syslog, API, custom software). Depending on the type of LTA in use, the LTA will reside either on the monitored Source, or on the Security Appliance.

"Notification" means an email to Client communicating the occurrence of an Incident or Security Incident.

"Notification Procedures" means documentation of how Clients will be contacted for different service scenarios. Notification Procedures are developed in collaboration with the Client during Transition.

"Security Appliance" means enablement of the Service by physical or virtual collection and forwarding of Logs for analysis.

"Standard Rule" means the standard rules dictating how the service will respond to the data within an Event.

"Source" means a device (for example, application, OS, database) that generates a Log, Event, report, or evidence used in the operation of the Service.

2. Service Scope

2.1 MSS Enterprise Security Monitoring is available in Standard or Enhanced Service Packages, consisting of the Service Features set out in the table below, and cannot be selected or deselected for a specific Configuration Item.

2.2 The Service Features common to all Managed Security Services listed in the table below are defined in further detail in *Part E. Common Service Features*. The Service Features specific to MSS Enterprise Security Monitoring listed in the table below are defined in further detail in clauses 4 to 9 inclusive.

2.3 Table of Service Features:

MSS Enterprise Security Monitoring Service Features	Service Package	
	Standard	Enhanced
Service-specific Service Features		
Security Appliance	✓	✓
Detection Type	✓	✓
Security Analyst Interaction	✓	✓
Access to Events and Incidents		✓

MSS Enterprise Security Monitoring Service Features	Service Package	
	Standard	Enhanced
Monitoring and Compliance Reporting		✓
Client Notification	✓	✓
Investigator Log Search Capability		Optional
Portal and Reporting	✓	✓
Common Service Features		
Security Incident Management	✓	✓
Availability Management	✓	✓
Event Management	✓	✓
Capacity and Performance Management	✓	✓
Service Asset and Configuration Management	✓	✓
Change Management	✓	✓
Request Fulfilment	✓	✓
Service Level Management	✓	✓

3. Service Exclusions

3.1 Dimension Data:

a. will not support altered, damaged, or modified software, or software that is not a supported version within the Service;

b. will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors), and the physical form factor if supplied by Dimension Data.

Service-Specific Service Features

4. Security Appliance

4.1 Dimension Data must gather Logs, Events, reports, and evidence data from in-scope Client devices and systems, then prepare the data for secure transmission and processing.

5. Detection Type

5.1 Dimension Data must use standard rule sets detection and compliance profile to identify and report on Security Incidents.

5.2 Dimension must ensure service quality by detecting tuning decisions based on the validity and relevance of Service-generated Events and Security Incidents on a continuous basis.

5.3 Dimension Data must use customised rules and an anomaly-based security detection and compliance profile to identify and report on Security Incidents.

5.4 Dimension Data must raise a Security Incident when:

a. there is a deviation from a predefined baseline definition of compliance controls; or

b. where there is a deviation from a pre-defined baseline of Client's custom business policy compliance requirements.

5.5 In addition to clauses 5.1 to 5.3 inclusive, if Client has purchased the *Enhanced* Service Package, Dimension Data must:

a. develop and implement up to 15 (fifteen) Compound Rules annually for Client; and

b. implement up to five (5) existing Complex Analysers annually for Client.

6. Security Analyst Interaction

6.1 If Client has purchased the *Standard* Service Package, Dimension Data must:

a. utilise automated detection for high confidence Security Incidents; and

b. ensure other Security Incidents are verified by a security analyst.

6.2 If Client has purchased the *Enhanced* Service Package, Dimension Data must ensure Security Incidents are verified by a security analyst.

7. Client Notification

7.1 Dimension Data must notify Client based on Client's selection of Notification options, for example via email or telephone.

8. Investigator Log Search Capability

8.1 If Client has purchased the optional *Investigator Search Log Capability* as part of the *Enhanced* Service Package, Dimension Data must provide Client with access to enriched and aggregated historical Log searches.

9. Service Portal and Reporting

9.1 Dimension Data must provide Client with access to standard reports via the Service Portal.

9.2 In addition to clause 9.1, if the Client has purchased the *Enhanced* Service Package, Dimension Data must provide Client with:

a. access to the previous ninety (90) days of Event and Security Incidents via the Service Portal; and

b. access to monitoring and compliance reporting.

Service-Specific Obligations

10. General Obligations

10.1 The Client must:

a. procure all maintenance, support, and licensing agreements with Third Party vendors for all non-Dimension Data provided in-scope devices for the term of the Agreement, unless otherwise stated in the purchase order;

b. work with Dimension Data to amend the purchase order accordingly if any devices are not compliant with the configuration guidance, including use of supported versions of Source devices only;

c. work with Third Party vendors to rectify device failure for all non-Dimension Data provided devices and be responsible for all associated expenses;

d. ensure compliance with all relevant data privacy, regulatory, and administrative policies and procedures related to monitoring of user traffic and communications;

e. notify Dimension Data and assist Dimension Data to identify and develop a mutually agreed mitigation plan if Client utilises security technologies that blocks traffic, rotates Logs, or otherwise impedes the ability of the Service to receive Logs from in-scope devices;

f. ensure the physical security of all Security Appliances located at Client Site or hosted at Third Party locations;

g. resolve Client Internet Service Provider (ISP) outages, or issues with Client internal network infrastructure; and

h. work with Dimension Data to amend the scope of work accordingly if:

i. regulatory changes (including, without limitation, changes by a regulatory agency, legislative body, or court of competent jurisdiction) require a modification to the Services described herein; and

ii. Client's environment generates an inordinate number of Logs or Events processed by the Service.

10.2 Dimension Data must raise a Security Incident when there is a deviation from a predefined baseline:

a. definition of compliance controls

b. of an organisation's custom business policy compliance requirements.

10.3 If Client has purchased the *Standard* Service Package, Dimension Data must use a standardised rule and anomaly-based compliance profile to identify and report on Security Incidents.

10.4 If Client has purchased the *Enhanced* Service Package, Dimension Data must provide customised compliance, security best practice and business policy enforcement monitoring requirements.

11. Access Requirements

11.1 The Client must:

a. be responsible for selecting Services and ensuring that the Service meets any and all compliance standards (for example, PCI, HIPAA) which apply;

b. assign a main Client Point of Contact (POC) to be available during all scheduled activities;

c. ensure that the assigned Client POC works with Dimension Data to schedule all Service-related activities and communicate with Dimension Data as needed for installation and ongoing tuning and support;

d. complete all reasonably required information for Transition in a timely manner;

e. notify Dimension Data in a timely manner of any changes to Client contacts for Security Incident escalation;

f. maintain Service Portal user list and rights;

g. provide access and connectivity to all Configuration Items, including the ability to receive Source feeds and evidence data including, without limitation, packet capture and stack trace;

h. provide knowledgeable technical staff, and/or Third Party resources, to assist with Hardware and Software implementations, including, without limitation:

   i. configuring end-to-end connectivity to ensure the successful transport of all in-scope Log feeds and evidence data;

   ii. providing rack space and power for each in-scope Security Appliance (if applicable);

   iii. providing an IP address for each Security Appliance to be installed at Client Site;

   iv. installing Security Appliances on Client network;

   v. installing Log Transport Agents (LTAs) in accordance with the instructions supplied by Dimension Data; and

   vi. working with Third Party vendors for support or provide authorisation for Dimension Data to contact Third Party vendors on behalf of Client as appropriate.

i. ensure Source device and LTA configurations comply with the standard setup requirements for the Service which will be made available during Transition; and

j. install, initially configure and enrol all Security Appliances in accordance with the guidance provided during Transition.

11.2 Dimension Data recommends that Client performs full backups of relevant systems prior to the performance of services.

11.3 If Client's configuration cannot or does not comply with configuration guidance, engineering consulting hourly rates will apply to develop a custom solution.

Appendix C. Scope of Service – MSS Security Device Management

1. Definitions and Interpretations

1.1 For the purposes of this Scope of Service, and in addition to the definitions in clause 1 of the Agreement:

"Co-Management" means Dimension Data and Client and/or its nominated Third Party(s) have access to in-scope Configuration Item(s) and the ability to make updates and configuration changes.

"Security Appliance" means enablement of the Service by physical or virtual collection and forwarding of Logs for analysis.

2. Service Scope

2.1 MSS Enterprise Security Monitoring is available in Standard or Enhanced Service Packages, consisting of the Service Features set out in the table below, and cannot be selected or deselected for a specific Configuration Item.

2.2 The Service Features common to all Managed Security Services listed in the table below are defined in further detail in *Part E. Common Service Features*. The Service Features specific to MSS Enterprise Security Monitoring listed in the table below are defined in further detail in clauses 4 to 10 inclusive.

2.3 Table of Service Features:

MSS Security Device Management Service Features	Service Package	
	Standard	Enhanced
Service-specific Service Features		
Health and Availability Monitoring • Monitoring • Improvement and Recommendation	✓	✓
Security Incident Investigation & Resolution • Security Incident Generation • Security Incident Diagnosis • Security Incident Resolution • Security Incident Reporting • Proactive Security Incident Response	✓	✓
Capacity Monitoring and Reporting • Capacity Monitoring and Reporting • Capacity Improvement Recommendation • Capacity Planning • Capacity Change Implementation	✓	✓
Asset Tracking and Reporting • Configuration Item Recording • Patches and Security Hotfixes • Major Version Upgrades • Signature Updates, Failures and Escalations • Backups	✓	✓

MSS Security Device Management Service Features	Service Package	
	Standard	Enhanced
Problem Management • Problem Identification and Recording • Solution Identification and Recording • Solution Implementation • Problem Reporting	✓	✓
Offsite Backup	Option	Option
Co-Management		Option
Common Service Features		
Security Incident Management	✓	✓
Availability Management	✓	✓
Event Management	✓	✓
Capacity and Performance Management	✓	✓
Service Asset and Configuration Management	✓	✓
Change Management	✓	✓
Request Fulfilment	✓	✓
Service Level Management	✓	✓
Service Level Management	✓	✓
Change Management	✓	✓
Request Fulfilment	✓	✓

3. Service Exclusions

3.1 Dimension Data will not:

a. provide Services for any devices not covered by a valid maintenance contract;

b. manage any devices where the Hardware or Software has been declared End-of-Life or end-of-support by the Manufacturer prior to the start of any Agreement or subsequent renewal period;

c. provide any services for expired software update subscriptions;

d. provide offsite storage of system backups;

e. replace obsolete Hardware or Software; and

f. implement changes for any capacity issues related to Hardware refresh or design.

3.2 Dimension Data will only be responsible for management and maintenance of the appliance software (in both physical and virtual form factors) and the physical form factor if supplied by Dimension Data.

Service-Specific Service Features

4. Health and Availability Monitoring

4.1 For applicable service levels and where Dimension Data does not have access to make changes, if Dimension Data makes recommendations to Client which have not been implemented and Configuration Item(s) create unacceptable levels of Events and/or Incidents (assessed by Dimension Data), Dimension Data reserves the right to disable the Health and Availability monitoring Service Feature recommendations have been actioned.

Monitoring

4.2 Dimension Data must:

a. monitor key performance indicators of Configuration Items' service state and resource utilisation to determine overall health, performance and availability;

b. ensure Incidents are automatically generated in Dimension Data's ITSM system based on Events which exceed thresholds against specific poll cycles of key metrics

c. ensure Events are investigated and analysed by an engineer who determines a potential corrective or control actions to resolve the related Incident; and

d. notify Client and keep Client up to date on issues with overall health and availability via the Incident ticket available on the Service Portal.

4.3 If Client has purchased the *Enhanced* Service Package and changes to Configuration Items are required, Dimension Data will follow the change management process.

Improvement and Recommendation

4.4 Dimension Data must:

a. utilise standard poll cycles and thresholds to baseline Configuration Items;

b. as a baseline is identified, adjust thresholds based on historical data collected to eliminate unnecessary Events occurring; and

c. utilise historical data to identify potential methods of improving Configuration Item performance and overall health and availability.

4.5 The Client must request customisation of thresholds through standard change management processes.

5. Security Incident Investigation and Resolution

Security Incident Generation

5.1 Dimension Data and Client must generate Security Incidents by raising a Security Incident-related ticket via the Service Portal or telephone.

5.2 Dimension Data must:

a. validate Security Incident tickets raised via the Service Portal and modify the impact and urgency if deemed necessary; and

b. create a Security Incident ticket on behalf of Client for Security Incidents raised via telephone, and assign the relevant impact and urgency.

Security Incident Diagnosis

5.3 Dimension Data must:

a. manage Security Incidents based on the Priority assigned to the Security Incident ticket raised;

b. calculate priorities based on impact and urgency of a Security Incident ticket;

c. ensure the Security Incident is triaged by the Service Operation Centre (SOC) to assess the Priority;

d. assign Security Incidents to the appropriate SOC engineer who will investigate and analyse further to identify a correction plan to resolve the Security Incident; and

e. provide Clients with Notification of updates to a Security Incident ticket via the Service Portal, and any restoration plan to resolve.

Security Incident Resolution

5.4 Dimension Data must:

a. work to resolve Security Incidents and move tickets to a 'resolved' state to allow the Client to confirm resolution; and

b. provide Client with updates on any Security Incident resolution plans via the Service Portal.

5.5 If the Client does not confirm resolution, the Security Incident will be automatically closed after 3 days.

Security Incident Reporting

5.6 Dimension Data must:

a. notify Client of all Security Incidents via a Notification email; and

b. make full details of the Security Incident available to Client via the Service Portal.

Proactive Security Incident Response

5.7 If Client has purchased the *Enhanced* Service Package, Dimension Data must:

a. proactively respond following detected Security Incidents, including when Security Incidents are escalated by the Service;

b. block specific communication-specifying elements, if necessary, after determination by a security analyst based on:

i. the specific elements that may include source and/or destination IP address;

ii. signature actions (e.g. Alert/block/reset); and/or

iii. user containment (limited to devices with AD integration).

c. obtain Client approval based on the response activity for a Configuration Item that involves a Service Request or Request for Change, if required; and

d. keep Client up to date with any response activity via the Service Portal and at its discretion via telephone calls to Client's security contacts.

5.8 Client must request cancellation of any communication blocked by a proactive response, if required.

6. Capacity Monitoring and Reporting

Capacity Monitoring and Reporting

6.1 Dimension Data must:

a. regularly check a number of telemetry points through continuous monitoring systems to highlight potentially impacting trends;

b. determine if there is a Problem that needs to be addressed or if Configuration Items are becoming oversubscribed, for example a disk filling with Log data;

c. liaise with Client to either resolve or mitigate identified risks;

d. utilise standard thresholds when gathering monitoring data, acknowledging that these thresholds may not be applicable to Client environment; and

e. liaise with the Client to adjust thresholds during Transition or after Service go-live where a baseline can be identified.

6.2 If thresholds are changed, Client must accept that this may result in unnecessary Events or false positives, and Dimension Data reserves the right to adjust thresholds accordingly.

Capacity Improvement Recommendation

6.3 Dimension Data must liaise with Client to determine the best plan and path forward when monitoring determines a Configuration Item is over-subscribed.

Capacity Planning

6.4 Dimension Data and Client must use trend data obtained as part of capacity monitoring and reporting to make decisions about future requirements and expected growth.

Capacity Change Implementation

6.5 If Client has purchased the *Enhanced* Service Package, Dimension Data must, through the consistent and uniform measurement of telemetry from Configuration Items, make recommendations or raise Requests for Change to be approved by Client to enhance or avoid future capacity issues that might arise, subject to the necessary approvals and advice being followed.

7. Asset Tracking and Reporting

Configuration Item Recording

7.1 If Client has purchased the *Enhanced* Service Package, Dimension Data must record and track Client Configuration Items and make this information available to Client.

Patches and Security Hotfixes

7.2 Dimension Data must:

a. monitor OEM-published patches, security hotfixes and version updates associated with Configuration Items and review such releases for applicability;

b. determine if updates or patches are recommended for security or operational reasons;

c. request approval from Client prior to implementing any updates through a request for change; and

d. install an unlimited number of qualified and applicable software patches and OS minor version upgrades for Configuration Items.

7.3 If Dimension Data determines that Client's Configuration Item is susceptible to a new low or medium vulnerability, Dimension Data will seek Client approval prior to taking any response steps. If a Dimension Data engineer deems a new vulnerability as high in severity, Dimension Data may take immediate response steps through an emergency Request for Change.

Major Version Upgrades

7.4 Dimension Data considers all major version upgrades as high risk as they pertain to Client's production environments.

7.5 Dimension Data must:

a. plan, coordinate, and manage all major version upgrades and roll-back options; and

b. coordinate all major version upgrades with Client and propose a fixed price project or perform the work on a time and materials basis at an Additional Charge.

Signature Updates, Failures and Escalations

7.6 Dimension Data must:

a. check that signature updates are being updated successfully where Configuration Item signature databases are automated and require connectivity between the Configuration Item and the internet to download items;

b. raise a Security Incident on behalf of the Client if signature updates fail;

c. resolve any errors related to a Configuration Item's ability to update signatures using the standard Security Incident management process; and

d. escalate to the Manufacturer on Client's behalf if the cause of the Configuration Item's inability to update signatures is an error or deficiency in the Manufacturer's database.

Backups

7.7 Dimension Data must:

a. retain a maximum of 7 (seven) previous full system Configuration Item backups onsite via the Security Appliance, subject to storage availability on the Security Appliance.

b. store 1 (one) offsite system backup and 1 (one) configuration backup where applicable, if Client has selected the offsite backup option;

c. store the last successful backup when a new backup cannot be obtained from the Configuration Item;

d. retain the last successful backup for 1 (one) year;

e. not make a configuration backup before a Request for Change is implemented and utilise the backup to roll back to the last known configuration in the event of a failure or request by Client; and

f. backup the following Configuration Item information (where applicable):

i. system configuration (operating system and configuration);

ii. configuration rules;

iii. signature configuration;

iv. signature pack;

v. configuration files;

vi. user database;

vii. operating system configuration; and

viii. management device configuration.

7.8 If Client has purchased the *Enhanced* Service Package, Dimension Data must:

a. maintain a backup of the Configuration Item system and configuration(s) in case of failure or where applicable unless defined as the Client's responsibility in this Agreement; and

b. backup the entire Configuration Item system every 24 hours.

7.9 If Client has purchased the optional *Co-Management* as part of the *Enhanced* Service Package, Dimension Data must ensure any change must explicitly request backup via a Service Request on the Service Portal, to ensure this will be completed. If the service is Co-Managed and a request is not made, Dimension Data may, at its discretion, roll back to the previous available backup and not be responsible for any previous changes lost or loss of Service as a result.

8. Problem Management

Problem Identification and Recording

Dimension Data's obligations

8.1 Dimension Data must raise a Problem record, where applicable, as a result of:

a. detection of a root cause of one or more Security Incidents that may or may not have a Permanent Resolution in place; and/or

b. analysis of available data to identify any trends which indicate that a Problem exists or is likely to exist.

8.2 Following the creation of a Problem record, Dimension Data will notify Client of the initial Problem classification and prioritisation.

8.3 Client may request the escalation of a Problem to a higher Priority by contacting an escalation manager through the Service Desk and quoting the reference number.

8.4 Dimension Data may downgrade an escalated Problem if it is being managed to a scheduled timeframe, or where a resolution has been provided to Client and is in the process of being tested.

8.5 Where Client initiated the escalation, Dimension Data will obtain Client's approval prior to downgrading.

Solution Identification and Recording

Dimension Data's obligations

8.6 Once a Problem record has been created, Dimension Data must:

a. investigate and determine the root cause of the Problem;

b. where possible, identify a Permanent Resolution to the Problem or a Workaround; and

c. update Client on progress.

Solution Implementation

Dimension Data's obligations

8.7 At Client's request, the recommended Permanent Resolution or Workaround will be coordinated and/or implemented by Dimension Data, whichever is applicable, depending on the scope:

a. where Client has procured the request fulfilment Service Feature, through remote fulfilment of Service Requests, as per the process set out in clause 8;

b. on a time and materials basis at an Additional Charge;

c. through a formal Consulting and Professional Services engagement, the scope and pricing of which will be agreed with Client and set out in a separate Scope of Service; or

d. in accordance with Dimension Data's obligations under an associated Service Feature which Client has procured.

Problem Reporting

Dimension Data's obligations

8.8 Dimension Data must provide Client with Problem management reporting information, including:

a. statistical information in respect of Problem management through the Service Portal; and

b. Problem management Service Level Target achievement.

9. Offsite Backups

9.1 If Client has purchased the optional *Offsite Backup* Service Feature, Dimension Data must:

a. store 1 (one) offsite system backup and 1 (one) configuration backup where applicable; and

b. retain the last successful backup for 1 (one) year where Dimension Data is unable to obtain a new backup from the Configuration Item.

10. Co-Management

10.1 If Client has purchased the optional *Co-Management* Service Feature as part of the *Enhanced* Service Package, Dimension Data must ensure that Client and/or its nominated Third Party have access to Configuration Items and the ability to make updates and configuration changes.

Service-Specific Obligations

11. General Obligations

11.1 If Client has purchased the *Enhanced* Service Package, the Client must:

a. notify Dimension Data in advance of changes being made to include scheduling and scope of changes to avoid “lost transaction” or collision of change work;

b. record all modifications to be made via a Request for Change;

c. make changes to a Configuration Item such that there is a clear audit trail indicating the Party responsible for the change, the date of the change and Client change control identification;

d. ensure that each change is made in such a way as to provide the possibility of rolling back to the previous version;

e. agree any changes to Dimension Data’s service administration rules with Dimension Data prior to their implementation;

f. acknowledge that any exception that may arise due to deviation from, or circumventing the processes described in this Agreement may result in unsecured device(s) and/or non-compliant configuration(s) and, accordingly, Client releases Dimension Data from any liability resulting from outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to changes implemented by Client or its Third Party(s);

g. ensure the physical security of all Security Appliances located on-site at Client locations or hosted at Third Party locations;

h. resolve Client Internet Service Provider (ISP) outages, or issues with Client internal network infrastructure; and

i. agrees in good faith to liaise with Dimension Data to amend the scope of work accordingly if regulatory changes (including, without limitation, changes by a regulatory agency, legislative body, or court of competent jurisdiction) require a modification to the Services described herein.

12. Access Requirements

12.1 The Client must:

a. ensure the Configuration Items under management for the duration of the Service have valid Manufacturer product license(s) required for all components (including security application and operating system);

b. ensure Configuration Items have full Manufacturer support at all times during the Term;

c. maintain all Manufacturer’s software subscriptions (software updates) for Configuration Items to be managed at all times during the Term;

d. ensure that only the manufacturer’s security application/operating system software, relevant and/or necessary software/applications and software provided by Dimension Data (where applicable) to support the Service are run on the Configuration Item;

e. implement a secure configuration policy, agreed between the Parties;

f. where applicable provide, monitor and support a virtual environment for the Security Appliance in accordance with the Security Appliance installation and configuration guide which is provided during Transition;

g. provide Dimension Data with full and exclusive administrative, root or read-write privileges for all Configuration Items for the duration of the Term;

h. facilitate the implementation of the Dimension Data Remote Management Kit (RMK), where appropriate;

i. assign a main Client Point of Contact to work with Dimension Data to schedule all Service-related activities and communicate with Dimension Data as needed for installation and ongoing support;

j. complete all reasonably required information for Transition in a timely manner;

k. notify Dimension Data in a timely manner of any changes to Client contacts for Security Incident escalation;

l. maintain Service Portal user list and rig agrees in good faith to liaise with Dimension Data to amend the scope of work accordingly if regulatory changes (including, without limitation, changes by a regulatory agency, legislative body, or court of competent jurisdiction) require a modification to the Services described herein;

m. provide knowledgeable technical staff, and/or Third Party resources, to assist with Hardware and Software implementations, including, without limitation:

   i. configuring end-to-end connectivity;

   ii. providing rack space and power for each in-scope Security Appliance (if applicable);

   iii. providing an IP address for each Security Appliance to be installed at Client site; and

   iv. installing Security Appliances on Client network; and

n. install, initially configure and enrol all Security Appliances in accordance with the guidance provided during Transition.

12.2 If Client has purchased the *Co-Managed* Service Feature as part of the *Enhanced* Service Package, and the Client disables such privileges either intentionally or in error, at any time, Dimension Data reserves the right to suspend the Service for the applicable Configuration Items until the situation is remedied. Dimension Data is not responsible for any Security Incident involving a Configuration Item while such privileges are disabled or otherwise non-functional.

Appendix D. Scope of Service – MSS Vulnerability Management

1. Definitions and Interpretations

1.1 For the purposes of this Scope of Service, and in addition to the definitions in clause 1 of this Agreement:

"Approved Scanning Vendor (ASV)" means an organisation with a set of security services and tools used to conduct external vulnerability scanning services to validate adherence with the external scanning requirements of PCI DSS Requirement 11.2.2. The ASV's scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC's List of Approved Scanning Vendors.

2. Service Scope

2.1 MSS Vulnerability Management consists of the Service Features set out in the table below, and cannot be selected or deselected for a specific Configuration Item. The Client acknowledges and agrees that Vulnerability Management does not include the performance of any penetration testing.

2.2 The Service Features common to all Managed Security Services listed in the table below are defined in further detail in *Part E. Common Service Features*. The Service Features specific to MSS Vulnerability Management listed in the table below are defined in further detail in clauses 4 to 14 inclusive.

2.3 Table of Service Features:

MSS Vulnerability Management Service Features	
Service-specific Service Features	
External Scanning	✓
Internal Scanning	✓
Self-Scanning	✓
Policy Templates and Customisations	✓
DHCP Support	✓
PCI Compliant Workflow	✓
Reporting	✓
Tuning	✓
Client Notification	✓
Portal and Reporting	✓
Common Service Features	
Security Incident Management	✓
Availability Management	✓
Event Management	✓
Capacity and Performance Management	✓
Service Asset and Configuration Management	✓
Change Management	✓

MSS Vulnerability Management Service Features	
Request Fulfilment	✓
Service Level Management	✓

3. Service Options

3.1 Dimension Data offers vulnerability scanning services through a combination of Service tiers, license levels, scan frequencies, and optional services, which determines the Service Features available to Client as described below.

MSS Security Device Management Service Features	Tier 1	Tier 2	PCI
Scan Configurations	1	8	1
Standard Reports	3	9	3
Custom Reports	0	2	0
SOC Scan Reviews	0	1	1
On-Demand Scans	0	0	1
Pre-Configured Assets	1	12	1
Discovery Scans & Report	1	1	1

3.2 Dimension Data must liaise with Client to set up scan configurations based on the Service tier selected.

4. Service Exclusions

4.1 Dimension Data will not:

a. be held liable for any outages affecting the Qualys service;

b. be responsible for any defect, fault, or impairment in the Service, notwithstanding anything to contrary herein, if such defect, fault, or impairment in the Services are caused by:

i. any breach by Client of any obligation hereunder;

ii. any negligent, fraudulent, or wilful act or omission by Client while using the Service or Dimension Data-provided equipment;

iii. any use of the Service, Dimension Data equipment or Dimension Data's network by an entity or person obtaining unauthorised access through Client; or

iv. any defect, fault or impairment in any Client equipment.

4.2 The Client must, at its expense, use commercially reasonable efforts to resolve, defects, faults, or impairments described in clause 4.1.

4.3 Qualys vulnerability management IP quantities are licensed and used based on unique visible IPs and or fully qualified domain names seen during vulnerability scans. Client cannot rotate IPs during the Term of the Agreement.

4.4 Any unused IP licenses at the end of the Term are not refundable.

Service-Specific Service Features

5. External Scanning

5.1 Dimension Data must specifically examine Client's security profile from the perspective of an external outsider.

6. Internal Scanning

6.1 Dimension Data must operate internal vulnerability scanning inside Client's firewall(s) to identify real and potential vulnerabilities inside Client's network.

7. Self-Scanning

7.1 Dimension Data must manage and execute scans if Client has not elected to do.

8. Policy Templates and Customisation

8.1 Dimension Data must create customised scanning templates for Client's environment.

9. DHCP Support

9.1 Dimension Data must provide Client with asset tracking over time, including in the event of changes to IP addresses.

10. PCI Compliant Workflow

10.1 Dimension Data must, as an approved Payment Card Industry Approved Scanning Vendor (PCI ASV) provide Client with a seamless end-to-end platform for all vulnerability management scanning needs.

11. Reporting

11.1 Dimension Data must make:

a. standard reports available to Client in line with the applicable Service tier; and

b. custom reports available using standard templates only.

12. Tuning

12.1 Dimension Data must liaise with Client to tune the vulnerability management systems in order to reduce the instances of false positives over time.

13. Security Analyst Review

13.1 A Dimension Data security analyst must carry out 1 (one) hour in depth scan status review, in line with the applicable Service tier.

14. Remediation Tracking

14.1 Dimension Data must provide Client with access to a dedicated portal so that it can track remediation workflow in a dedicated portal.

Service-Specific Obligations

15. General Obligations

15.1 The Client must:

a. own, manage, or control the IP address range(s), internet-accessible IPs, and internet-accessible devices in-scope;

b. notify Dimension Data at least 24 hours prior to the scan start if Client wishes to request changes to any managed scan configuration defined within a specific service tier (described in clause 3.1);

c. notify Dimension Data at least 24 hours prior to the scan start;

d. provide accurate metrics so that Dimension Data purchases a correct Qualys licence. If it is determined later an incorrect license was attributed to Client based on inaccurate information, it will be Client's sole responsibility for any additional charges;

e. accept that:

i. license true up activities and any data purges as a result are a function of the Qualys SaaS service; and

ii. solution recommendations are made by Qualys alone and are performed at the discretion and risk of Client. Dimension Data is not responsible for damages resulting from Qualys' solution recommendations and suggests that all systems have proper backups prior to implementing any remediation.

f. not hold Dimension Data liable for damages because of any internal, external, or agent based Qualys scan;

g. acknowledge that:

i. scanning may be disruptive to an environment and could result in denial of Service, data and or system corruption, loss of data, system crashes or the general performance and availability of systems; and

ii. Qualys does not guarantee to find all vulnerabilities, does not perform web application assessments and does not guarantee the absence of false positives;

h. not modify any standard report or reporting template;

i. be responsible for all relevant data privacy, regulatory, and administrative policies and procedures related to monitoring user traffic and communications; and

j. agrees in good faith to liaise with Dimension Data to amend the scope of work accordingly if regulatory changes (including, without limitation, changes by a regulatory agency, legislative body, or court of competent jurisdiction) require a modification to the Services described herein.

15.2 Dimension Data reserves the right to run discovery scans at its sole discretion to enable validation of the scope and license(s) or assist in validating other concerns that either Client or Dimension Data may reasonably have before an assessment starts.

15.3 Dimension Data will configure the scanning system with the appropriate IPs and scan configurations as defined by Client's Service tier. Each scan start time will be in accordance with a Client Service profile to be agreed between the Parties.

15.4 Dimension Data will configure the number of assets defined by the Service tier for the purposes of scanning, reporting and remediation.

15.5 Dimension Data will monitor license quantities and regularly communicate these to Client. Any overages at the end of the standard yearly contract cycle will be billed to Client at the rate set out in this Agreement.

16. Access Requirements

16.1 The Client must:

a. be responsible for selecting Services and ensuring that the Service meets any and all compliance standards (for example, PCI, HIPAA) which apply;

b. assign a main Client Point of Contact (POC) to be available during all scheduled activities;

c. ensure that the assigned Client POC works with Dimension Data to schedule all Service-related activities and communicate with Dimension Data as needed for installation and ongoing tuning and support;

d. ensure access and connectivity to all Configuration Items within the IP address ranges(s) and internet-accessible IPs considered in-scope for the Service; and

e. provide knowledgeable technical staff, and/or Third Party resources, to assist with Hardware and Software implementations, including, without limitation:

i. notifying Dimension Data of any potential problem areas, which could interfere with scanning activities, such as load-balancing;

ii. resolving Internet Service Provider (ISP) outages and internal network infrastructure issues;

iii. ensuring information provided to Dimension Data is accurate (for example, web site banners, Hardware, Software, operating system and application versions) to allow Dimension Data to properly validate vulnerabilities for PCI ASV dispute resolution; and

iv. notifying Dimension Data of any new Configuration Items substituted into “in scope” IP address ranges.

16.2 If Client elects to receive Approved Scanning Vendor (ASV) PCI Services, Client agrees to be bound by the terms and conditions of the then current version of the PCI DSS Validation Requirements for ASVs set forth by PCI Security Standards Council (https://www.pcisecuritystandards.org/).

16.3 Client must follow each payment card company’s respective compliance reporting requirements to ensure Client’s compliance. While scan reports must follow a common format, the results must be submitted according to each payment card company’s requirements.

16.4 For PCI ASV scanning, Client is required to white list NTT Security (on behalf of Dimension Data) and Qualys scan ranges through the Client’s DMZ in accordance with the then current PCI ASV Program Guideline rules (https://www.pcisecuritystandards.org/).

16.5 In the event that Client utilises IPS auto-shunning technology, proxy firewalls such as VelociRaptor®, defense mechanisms such as SynDefender®, or the PIX® TCP Intercept feature (or similar technologies), Client must implement one of the following to ensure Dimension Data can produce accurate scanning results:

a. appropriately configure router Access Control Lists (preferred method);

b. configure Configuration Items to monitor and log, but not block Dimension Data’s incoming IPs;

c. interface filters directly on the firewall; or

d. disable this feature for Dimension Data's scanning IP(s).

16.6 If Client needs to substitute in scope IPs, Client agrees in good faith to liaise with Dimension Data to amend the scope of work accordingly.

16.7 If load balancing is in use, Client must provide Dimension Data with written assurance the infrastructure behind the load balancers is synchronised in terms of configuration. If Client fails to provide written assurance, PCI Security Standards Council requirements state Dimension Data must individually scan the components from an internal location within Client's environment. If internal scanning is required, Dimension Data will work with Client to amend the scope of work accordingly.