1. Service Overview

Our Managed SD-WAN provides a secure, encrypted overlay network for connecting your HQ, data centres, branch offices, endpoints and workloads (located in private and public cloud environments) to each other.

The Service provides secure controlled access to SaaS based applications hosted on the internet, secure firewalling and next-generation features. It provides automated network traffic reporting and access to a single view of the SD-WAN Estate.

Our Managed SD-WAN Service is deployed in Hub and spoke network configuration, provided via either the managed connectivity services provided by us or your own connectivity services, typically over the internet. We deploy the Service in various ways:

(a) via a new connectivity deployment with us;

(b) via a pre-existing connectivity deployment with us; or

(c) via third party internet connectivity.

Our SD-WAN Service may be deployed for access in the UK, Europe or internationally. If specified, we can configure the Service to operate over diverse types of access networks including 4G/5G and broadband or fibre leased lines. We can configure over single or multiple network connections, using single or dual SD-WAN MSDD or so as to terminate network connections directly via the SD WAN MSDD or behind a pre-existing service you are procuring from us or from a third party.

2. Service Features

We offer two managed service tiers as part of our SD-WAN Service:

(a) Essential; and

(b) Advanced

Your choice of Service tier per site will be specified on your Order Form and/or Statement of Work. The tables below detail the features offered as part of each tier which are cumulative. Essential delivers the specified core features. The Advanced Service tier offers all of the features of both Essential and Advanced tiers.

2.1 SD-WAN Essential

Feature	Description
Encryption	Secure IPSec Encrypted network over our NGN-Internet/Managed WAN or via a third party.

Access to Multi- tenanted Infrastructure	Resilient design of SD-WAN infrastructure.
Single or Resilient deployment	Single or Resilient managed device deployed to site depending on your requirement(s).
Application Aware Prioritisation	Flexible application-based policies configured for your business environment and applied across your estate. Application Aware Prioritisation is used as part of the SD-WAN Service. As default we will implement a SD-WAN Standard policy that will favour voice, video and network control policies over other traffic on the line. Policies can be requested to suit your requirements including additional application-based policies and support of traditional QoS mappings (DSCP across existing MPLS).
Active-Active	SD-WAN allows your traffic to pass over a single or multiple underlying network connections. Traffic can be steered over connections based on application type, usage or network status and use both connections simultaneously. Traffic can be configured to automatically fail-over to another connection in the event that the line(s) fail. Your requirements will be captured in your Statement of Work.
Smart Secure Local Breakout	Optimised local site SaaS internet breakout which enables efficient routing to the internet to provide local breakout on sites that traverse internet lines. This feature allows for the detection of defined public SaaS traffic and route it out locally to enable the most efficient routing to the internet. Full local breakout is not in scope of this feature.
Remote User VPN	Connect your users securely regardless of location via a client on their Windows or MacOS devices (mobile and tablet devices are not included). This feature includes integration to your Active Directory for role based access control. It also includes support for integration into your own two factor authentication. Remote user VPN includes a pre-authentication check to validate the presence of anti-virus software, a Firewall or both.
Automated Reporting	Automated network status reports emailed to the contacts specified by you on a weekly basis. Further information can be found in Section 5.9.
Consolidated view of Estate	You will be provided with access to a read-only portal view of your SD-WAN Estate allowing visibility of the up/down status across all devices, Packet Loss and Jitter.
Managed Maintained Hardware	The SD-WAN MSDD is owned, managed and maintained by us throughout the life of the Service. We will maintain it in situ and if we cannot ensure that normal Service is restored with the SD-WAN MSDD, we will replace it with the same or equivalent model. Further information can be found in Sections 5.5 and 5.7.
Central Policy Management	SD-WAN provides a central Management Platform for security policy management enabling group-wide policy changes to be viewed and pushed out across multiple devices from one place.
VLAN	Up to seven (7) VLANs can be separated across your SD-WAN Estate to provide segmentation. VLANs will be replicated across each DW-WAN estate site.
Traffic Policy	Allows the control of traffic flow between critical and non-critical network segments across your network.
Logging	Three (3) weeks' worth of Syslog log retention of your SD-WAN Estate. Logging is stored on the UK based cloud platform owned and operated by us and hosted on our network accessible via the SD-WAN Management Platform.

Site Groups	One Site Group is delivered as standard across all tiers, with additional groups available to support segmentation of a wide area network within the SD-WAN Estate, enabling additional grouping control of traffic (e.g. separate business units requiring different rule or traffic flows). Site Groups are charged as a monthly recurring Fee for each group.

2.2 SD-WAN Advanced

Feature	Description
Logging	A total of six (6) weeks' worth of Syslog log retention of your SD-WAN Estate. Logging is stored on the UK based cloud platform owned and operated by us and hosted on our network accessible via the SD-WAN Management Platform.
Secure Local Internet Breakout	Provides secure access to the internet via Next Generation Firewall Functions within the SD-WAN MSDD.
Inbound Services	This feature provides: • inbound and outbound policy rules to segregate traffic; • inbound file blocking based on type of unencrypted traffic; • inbound NAT devices hosted within the LAN estate (e.g. CCTV or door entry systems where one policy is used for the entire Site Group); and • Five (5) VPN connections to external organisations via IPsec which is not part of the SD-WAN overlay.
Intrusion Prevention System	Intrusion Prevention System (IPS) to protect your environment from network-borne attacks. Your SD-WAN MSDD has two techniques to deal with these attacks: anomaly and signature-based defense.
URL Filtering	Our SD-WAN URL filtering feature is designed to restrict or control the content able to be accessed, delivered over the internet via a web browser. Our filtering solution utilizes three main components of the web filtering function: the web content filter, the URL filter and the Fortiguard Web Filtering service.

2.3 Additional Services

We offer the following additional services to complement our SD-WAN Managed Service. These can be requested separately and are subject to an additional Fee. Your selection will be indicated in your Oder Form and/or SoW.

Feature	Description
Pen Test	We carry out a penetration test of an external facing SD-WAN IP address and provide you with a report of our findings.
SD-WAN Readiness Assessment	We carry out an internal LAN security scan of your existing environment(s). This scan is run over three (3) to five (5) days. We will provide you with a report of this scan and we will use this to help you understand your environment(s).
Secure Advanced Remote VPN	Continued end point management and protection regardless of access to the internet. Secure advanced remote VPN allows your IT department to maintain a view of end point devices and apply governance and control.
Dedicated Management Infrastructure	Dedicated management platform, rather than the use of shared platforms. All management platforms are operated on our own cloud infrastructure. The applicable Fees will be set out in your Order Form.

	Such Fees will cover licensing, disk, CPU, RAM, patching and our day-to-day operations. Please note that we will maintain logging and analytics on our share systems.
LAN switching and wireless access points	LAN switching and wireless access points controlled by the SD-WAN MSDD to support branch office locations, which we will configure as part of the solution design. The Fees for the hardware, software support, hardware replacement and replacement SLAs with be set out in your Order Form. We will support and manage these devices in accordance with the Managed Network Device Service Description included in your Order Form.

2.4 Access Services

If SD-WAN Managed Service is purchased with our Access Services, by default we will deliver them as a DIA (Dedicated Internet Access) Service.

If you specify it, the Service can be deployed using our Managed WAN Service or third-party connectivity. The management of any third-party connectivity is outside the scope of this Service.

3. Service Implementation

After order acceptance, we will implement the Service as follows:

Service Implementation	Us	You
We will agree the relevant resources and contacts for successful project completion.	•	•
We will hold a project initiation meeting to agree milestones and timelines with you.	•	•
We will send a welcome pack to you and confirm details captured in the SD-WAN design process.	•	
You will advise us if there are any site-specific access requirements, processes or contacts to facilitate the installation of the Service.		•
We will place the orders with our third party suppliers to fulfil the Access Service(s).	•	
We will schedule site surveys with you, where required.	•	
We will confirm any additional work required following the site survey(s).	•	
We will confirm your commit date(s) with you.	•	
We will pre-configure and dispatch routers to your preferred address(es).	•	
We will install Access Service(s) for you.	•	
We will confirm the Ready for Service Date with you and provide you with our handover documentation.	•	
We will jointly activate the Access Service(s).	•	
We will add the device to your SD-WAN Estate management portal and complete your configuration.	•	
We will test your Access Circuits to confirm performance, Latency, Packet Loss and throughput are as expected.	•	

You will confirm that the SD-WAN MSDD is connected to your LAN.		•
If multiple Access Services are provided, we will confirm correct operation of failover and application steering is tested in conjunction with your site contact.	•	•
We will demonstrate the Service to you.	•	
You will check and confirm access and visibility of your IT resources over the new Service.		•

Unless otherwise agreed with you, all implementation work will be carried out during Business Hours. We will invoice additional charges for any work undertaken out of hours. We reserve the right to charge additional Fees in accordance with your MSA for any change in your requirements occurring after the implementation of the Service and outside the scope of the contract.

3.1 Ready for Service

If the SD-WAN Service is being delivered in combination with an Access Service that we provide, the Ready for Service Date will be the date when we notify you that the SD-WAN MSDD and the Access Service are both operating and capable of being activated to carry live traffic.

If the Service is being provided using a third-party access service, the Ready for Service Date is the date when we notify you that delivery of the SD-WAN MSDD (as far as is reasonably achievable) is completed so that it could be activated on that third-party Service (whether or not the third-party Service has been delivered).

If you are unable to allow access to your site for the activation of your SD WAN MSDD, the Ready for Service date will be five (5) days after we provide you with notice that the site is ready for activation.

For Resilient Access, the Ready for Service Date of one Access Service may differ to the Ready for Service Date of another Access Service. By default, unless specified otherwise in your Statement of Work, we will bill each component separately. We will bill each component as it becomes Ready for Service. For example, if the secondary service is ready for use before the primary service, we will commence billing on the secondary element.

4. Billing

The Service will be billed as Recurring Fees as described in the Billing Guide, using the definition of the Ready for Service Date in Section 3.1 of this Service Description.

5. Service Operations

You can log and track all of your requests on our client portal. We will provide you registration and login details during the Service Implementation phase.

Our support team can be contacted by phone, email or via our client portal and will be able to assist you with the following:

(a) Change enablement;

(b) Incidents;

(c) Ticket updates;

(d) Portal logins;

(e) Service reporting; and

(f) General queries.

When you contact our support team, we will issue you with a reference number which acts as your unique reference for your incident or request. We will ask you to quote this reference number when contacting the support team to provide information or an update.

5.2 Incident Management

Our support team can be contacted by phone, email or through our client portal to report an incident relating to your SD-WAN Estate.

During the triage process, the incident priority may be adjusted based on the incident classification definition in Section 10.

We will provide updates through our client portal until the incident is resolved, and the ticket is closed.

5.3 Event Management

We provide proactive monitoring and support for the Availability of the SD-WAN Managed Service. Details of event monitoring, thresholds and alerts are included in our event management matrix, a copy of which can be provided upon request.

As part of a HA configuration, the SD-WAN MSDD is continuously testing the quality of the lines with IP SLA probes to indicate if traffic can be passed. Should an issue be detected an alarm will be received into our support team.

Our support team will then commence its incident management process. Our demarcation point will be the ports facing your equipment (typically the LAN ports on the SD-WAN MSDD).

If you have an issue which generates alerts and you do not resolve it based upon our reasonable advice within twenty-four (24) hours from being notified to do so, we reserve the right to disable alerting and will not be liable for any interruptions to your organisation.

5.4 Service Request Entitlement

A service request for an SD-WAN Essentials site is defined as one (1) request of the items listed in the tables at Sections 5.4(a) and 5.4(b) below.

As standard, we offer up to five (5) service requests per month free of charge via a fair usage policy for the Essentials tier and up to ten (10) service requests per month free of charge for Advanced. We can implement additional service requests as and when required and may charge additional fee for which will be defined in your Order Form or SoW. Any service request

that is not specifically defined in the tables at Sections 5.4(a) or 5.4(b) below will be considered a professional services engagement subject to an additional Fee calculated on a time and materials basis. These changes must follow the process covered in our MSA.

We will implement standard service requests listed in the tables below in accordance with the resolution times for priority 4 tickets as listed in Section 10.

Service requests are subject to our fair usage policy. You can request a specific volume of each request deemed to be a standard service request in a calendar month. The maximum volume of each request that you can request is set out in the tables below.

(a) SD-WAN Essentials

The SD-WAN Essentials includes up to five (5) service requests per month free of charge.

Service Request	Description	Volume per request (fair use per month)
Firewall Policy Rule	Amend Firewall policy rules for external and internal access through the SD-WAN MSDD.	Up to 5 rules
Firewall Objects	Add Firewall object to a defined policy rule.	Up to 5 rules
LAN port changes	Amendments to SD-WAN MSDD ethernet ports and VLAN that face your LAN.	1 port change
SD-WAN overlay and Smart Secure break out	Addition or change to Smart Secure internet breakout, such as addition of Teams, Office 365 or other SaaS service to the local breakout. Addition or change to rule of the SD-WAN overlay policy.	1 rule change
Routing changes	Add or modify an internal/external routing change affecting single/multiple destinations.	Up to 5 changes
LAN IP Address changes	IP changes to the ethernet ports that face your LAN.	1 change
DHCP scope changes	DHCP scope changes to the SD-WAN MSDD.	1 change
DHCP relay address changes	DHCP relay address changes on the SD-WAN MSDD.	1 change

(b) SD-WAN Advanced

The SD-WAN Advanced includes up to ten (10) changes per month free of charge.

Change Request	Service Request	Volume per request (fair use per month)
Firewall policy rule	Amend Firewall policy rules for external and internal access through the SD-WAN MSDD.	Up to 5 rules
Firewall objects	Add Firewall object to a defined policy rule.	Up to 5 rules

URL filtering	Modification to a defined URL filtering list.	Up to 5 rules
LAN port changes	Amendments to SD-WAN MSDD ethernet ports and VLAN that face your LAN.	1 port change
SD-WAN overlay and Smart Secure break out	Addition or change to Smart Secure internet breakout, such as addition of Teams, Office 365 or other SaaS service to the local breakout. Addition or change to rule of the SD-WAN overlay policy.	1 rule change
Routing changes	Add or modify an internal/external routing change affecting single/multiple destinations.	Up to 5 changes
LAN IP address changes	IP changes to the ethernet ports that face your LAN.	1 change
DHCP scope changes	DHCP scope changes to the SD-WAN MSDD.	1 change
DHCP relay address changes	DHCP relay address changes on the SD-WAN MSDD.	1 change

5.5 Maintenance, Patching and Management

The SD-WAN MSDD is owned, managed and maintained by us during the life of the Service. We will maintain it in situ (this could be a firmware upgrade/reboot). If we cannot ensure that normal Service has resumed with the SD-WAN MSDD, we will replace hardware with the same or equivalent model.

All SD-WAN MSDDs are installed with the current approved firmware as defined by our engineering team.

We will review your estate quarterly and check that patching is aligned to our recommended baseline. Where patching is required, we will arrange a maintenance window to carry out the work.*

The applicable MSDD will require a hardware refresh if the hardware is forecast to reach the end of vendor's support after the end of your Initial Service Term. Hardware refresh is outside the scope of this Service and is a chargeable activity.

We will identify and validate vulnerability with Critical and High severity (CVSS 3.0 7.0+) in the deployed firmware and evaluate the applicability of such vulnerability. If exploitable, we will remediate Critical (CVSS 9.0+) vulnerabilities within fourteen (14) days from our assessment, and High (CVS7,0+.) vulnerabilities within thirty (30) days. Critical-severity vulnerabilities that cannot be remediated without interruption to your Service will require emergency maintenance, for which we may not be able to provide advanced notice of any service interruption, especially if it is reported that the vulnerability is already being exploited by threat actors. If we become aware that a specific critical vulnerability is being maliciously exploited anywhere in the world, we will use reasonable endeavours to remediate such vulnerability within two (2) Business Days of our initial assessment, provided that the vendor has made available an updated software version or alternative remediation is technically possible.

*Please note that, if you are unable agree a maintenance window with us for a scheduled patch update following our notification, we cannot guarantee the patching will take place in the above timeline.

5.6 Platform Maintenance, Patching and Management

Shared and/or dedicated management platforms are also owned, managed and maintained by us during the term of your Service. We will carry out maintenance and patching during Business Hours as changes to your management platforms does not affect live traffic.

We will apply patching and software revisions in line with the approach described in Section 5.5.

5.7 Hardware Replacement

The SD-WAN Service includes hardware replacement of the SD-WAN MSDD. In the event of a service affecting failure, we will arrange for replacement hardware to be delivered to you.

For Essentials, we will endeavour to deliver a replacement on the next Business Day to UK locations, providing that the fault is diagnosed prior to 12pm. For Advanced, we will endeavour to deliver a replacement to UK locations within seven (7) hours of the fault being diagnosed. Response and delivery times to locations outside of the UK can be provided on request.

5.8 Service Delivery Management

The Service Delivery Management ("SDM") team will perform virtual quarterly service review meetings. These reviews will provide service governance and review the performance of your Service.

A typical agenda for the regular service review would be:

(a) Actions from previous meeting;

(b) Performance review;

(c) Monthly performance against SLA;

(d) Incident/RITM volumes and trends;

(e) Monthly ticket closure report;

(f) Problem tickets;

(g) Recommendations based on outputs from incidents or problems;

(h) Major incident reporting including root cause analysis;

(i) Frequency and cause of recurring incidents;

(j) Current changes or future planned changes;

(k) Billing;

(l) Review of any risk or problem logs;

(m) Service Credits (if applicable);

(n) Product updates and news;

(o) Key contacts;

(p) Escalation matrix; and

(q) NPS.

Your SDM will provide a reporting pack at least two (2) Business Days before your scheduled service review. Your SDM will capture all minutes and actions and will share the meeting minutes no later than two (2) Business Days following the review.

The SDM also provides you with a single point of contact and escalation to assist with any questions you have outside of service operations.

5.9 Automated network reporting

You will receive automated network status reports on a weekly basis which will be emailed to your selected contacts. The report will show the following:

(a) Traffic;

(b) Sessions;

(c) Top applications by bandwidth and sessions;

(d) Top users by bandwidth and sessions;

(e) Top destinations by bandwidth and sessions;

(f) Traffic history by user volume;

(g) SD-WAN VPN usage;

(h) System events by data and severity;

(i) Latency and Jitter measured to designated SaaS or internal services; and

(j) Packet Loss across link and SD-WAN tunnel.

6. Exit Assistance

As a standard, we will perform the following activities shortly before or upon termination of your Service:

(a) We will confirm your termination dates and site locations that will be terminated;

(b) We will provide details of the MSDD returns process;

(c) We will delete relevant data on the target site via the SD-WAN management portal (please note that this process is irreversible once initiated); and

(d) We will delete all of your backup data, related components and the environment.

Please note that it is your responsibility to provide a valid termination notice in accordance with the terms of your MSA. We reserve the right to charge additional Fees for the performance of the activities listed above if you fail to provide such notice.

If you require us to perform any activities in addition to those listed above, we can provide professional services subject to an additional Fee.

7. Dependencies

We provide the SD-WAN Service subject to the following dependencies:

7.1 Client Obligations

(a) You will designate a project lead and technical contacts with the appropriate level of expertise to support the successful implementation and operation of the Service;

(b) You will provide us with all of the information needed to complete the configuration of the Service. Once we have this information, we reserve the right to charge further Fees should there be any changes to your requirements;

(c) You will manage any of your own third parties needed during Service Implementation or Service Operations. We reserve the right to charge further Fees should you require us to manage your third parties;

(d) You will provide us or our third parties with access to your site(s) for set up and maintenance of the Access Service and for maintenance of the SD-WAN MSDD. We reserve the right to charge further fees should you require us to manage your third parties;

(e) During the installation of the Service, it is your responsibility to show our installation engineer (or our third-party engineer) to the installation point;

(f) You will ensure that structured cabling and appropriate LAN connectivity are in place on your site(s);

(g) You will provide Comms Room space in your site(s) for the SD-WAN MSDD and we will minimise downtime as far as reasonably practical.

7.2 Prerequisites

You are responsible for ensuring that the items below are in place:

(a) An Access Service provided by us, either through our DIA or Managed WAN services, or a third party provided access service;

(b) Adequate AC power to support each device, one (1) socket per device up to maximum of four (4);

(c) Adequate airflow to enable devices to operate correctly;

(d) Adequate space to safety house the devices to prevent damage to the device;

(e) Carry out first line checks as requested by our Service Desk; and

(f) You will are responsible for providing reasonable assistance to enable us to undertake planned maintenance on the SD-WAN MSDD following written notification. We will provide you with no less than twelve (12) Business Days' notice.

7.3 Service Dependencies

(a) If the firmware of your MSDD is forecast to become EoL during a new / refreshed contract term, we will no longer be able to provide security or critical firmware updates. In order to continue to receive security and critical updates, a hardware refresh of the MSDD will be required. Please note this hardware refresh (e.g. providing a new MSDD) is outside the scope of this Service and will be at cost to you. If needed, we will provide a new MSDD to you for an additional Fee;

(b) (c)(d) Please note that we require an active licence with the relevant vendors MSDD to be able to apply patching in accordance with Section 5.5. If such licence is not in place, we will use reasonable endeavour to patch your MSDD, but our ability to apply patching may be limited

8. Exclusions

The excluded items described below are outside the scope of this Service Description:

(a) Where the underlying Access Circuits are not provided by us, you will be responsible for reporting circuit issues to your third-party provider;

(b) We are not liable for any issues relating to your third-party provider; and

(c) Any activities other than those specifically set out in this Service Description.

9. Definitions and Acronyms

9.1 Definitions

In this document "we" or "us" refers to the Supplier, and "you" refers to the Client.

The terms listed have the following definitions:

Term	Meaning
Active Directory	Microsoft's Active Directory product - a directory service.

Access Circuit	A dedicated Broadband or Ethernet connectivity circuit connecting your site to one of our core network Points of Presence (PoPs) or the Internet.
Access Service	Please refer to Section 2.1 Access Service in either our DIA or Managed WAN Service Description.
Application Aware Prioritisation	The ability for the SD-WAN MSDD to be able to identify traffic based on application type and choose which link to use. Link usage is calculated by the use of IP SLA.
Availability	The ability to transmit a 64-byte IP data packet from the SD-WAN MSDD to the Designated Reference Router over the active Access Service whilst not Congested.
Comms Room	A communications room, usually air-conditioned, devoted to the continuous operation of computer servers.
Congested	Where the utilisation of the available bandwidth is greater than 75%.
Dedicated Management Infrastructure	A Management Platform (as described below) with some or all portals dedicated to the management/monitoring of an individual customer.
Designated Reference Router	Any designated SD-WAN MSDD within your SD-WAN (e.g. the SD-WAN MSDD on your Headquarter Site) or, where there is no other SD-WAN MSDD within the SD-WAN or when the Access Service to the designated SD-WAN MSDD has a Fault/is Congested, the Provider Edge Router in our NGN.
DSCP	Differentiated Service Code Point. A method of mapping data types to specific queues for prioritisation as part of QoS functions.
DDoS	Distributed Denial of Service attack A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. a DDoS attack is like an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.
DHCP	Dynamic Host Configuration Protocol is a client/server protocol which automatically provides an Internet Protocol (IP) with its IP address and other related configuration information such as the subnet mask and default gateway.
Firewall	A device designed to block unauthorised access while permitting outward communication.
FortiGuard Web Filtering	Fortinet's (third-party supplier) web filtering product.
High Availability	High availability is SD-WAN MSDD devices deployed as a pair to maintain Service in the event of an individual failure.
Intrusion Prevention System	A network security service that continuously monitors network traffic for malicious activity and takes action to prevent it.
IPsec	Internet Protocol Security is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure and encrypted communication between SD-WAN MSDD and the SD-WAN headed devices over a wide area network or the public Internet.
Jitter	The variation in latency of a 64-byte IP data packet from the SD-WAN MSDD to the Designated Reference Router over the active Access Service whilst not Congested, or vice versa, whichever is the greater.

Latency	The round-trip time in milliseconds it takes for an ICMP packet to traverse from your site SD-WAN MSDD to our Core Network.
Management Platform	Our portals used to operate, manage and report on all SD WAN MSDDs.
MPLS	Multi-Protocol Label Switching – used to provide an organisation with a private segregated network over a shared service provider infrastructure.
MSDD	Managed Service Demarcation Device, marking the handover of the Service from us to you.
Next Generation Firewall Functions	Deep Packet inspection, Intrusion Protection and threat detection, URL Filtering, SSL decryption.
PA IP Space	Provider Aggregable IP space. Space that is loaned to an organisation that does not have PI space from their Service provider. This IP space is returned at the end of the contract.
Packet Loss	The percentage of packets of actual traffic not delivered from the SD-WAN MSDD to the Provider Edge Router over the active Access Service whilst not Congested, or vice versa, whichever is the greater.
PI IP Space	Provider Independent IP Space assigned to an organisation by a Regional Internet Registry (RIR). The organisation can move this from one Service Provider to another.
PoP	Point of Presence, physical location providing network connectivity and services.
Primary Access	A single access service used as the default service in either a standard or resilient service.
Protected Access	Two Access Services which are provided with different types and bandwidth with Primary Access using Fibre and Secondary Access using a broadband service.
Provider Edge Router	A PER is router between one network service provider's area and areas administered by other network providers.
Resilient Access	Both primary and secondary access services are used and configured in an active/passive set-up whereby the primary Access Service is used by default. If the MSDD router detects an issue with the primary Access Service, the secondary Access Service is automatically used until the MSDD router detects that the primary Access Service is re-established.
SaaS	Software as a Service. Typically, accessible directly over the public Internet, such as Office 365, Salesforce.com, Amazon Web Services.
SD-WAN Estate	Includes all SD-WAN MSDD and Head-end devices within your VDOM and SD-Branch where additionally purchased.
SD-WAN Head-end Devices	Multi-tenanted Highly Available SD-WAN network hosted Firewalls, these devices are owned, managed and operated by us. They form the central Hub for your SD-WAN network and will terminate the IPsec tunnels that connect sites together and access IT.
SD-WAN MSDD	Six Degrees owned and operated Managed Service Demarcation Device which is leased to you, configured to participate in a managed SD-WAN Overlay network. The SD-WAN Managed Service Demarcation Device marks the handover of the Service from us to you.
Secondary Access	A second access service that is used when an issue is detected with the primary access service.

Site Group	A collection of SD-WAN MSDD's that adhere to the same Firewall inbound and outbound rules to allow users to access application or services such as CCTV, Web Servers, Door access system.
Six Degrees Next Generation Network or "NGN"	Our core network - owned, operated and managed by us.
Smart Secure	As defined in Section 2.1.
Standard Access	A single Access Service provided from your site to one of our PoPs.
Standard Access-Broadband	A single Access Service using standard broadband connectivity such as ADSL, FTTC, SOGEA, FTTP or wireless connectivity, provided from your site to one of our PoPs.
Statement of Work	A document which defines project-specific or client-specific activities, deliverables and/or timelines for providing services to that client.
Syslog	A standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyses them. This data is used to compile weekly automated email reports and for retrospective analytics.
VDOM	A VDOM provides separate security domains that allow separate zones, user authentication, Firewall policies, routing, and VPN configurations.

9.2 Acronyms

Acronym	Meaning
ADSL	Asymmetric Digital Subscriber Line
EoL	End of Life
FTTC	Fibre to the Cabinet
FTTP	Fibre to the Premise
HA	High Availability
HQ	Head Quarters
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching
MSDD	Managed Service Demarcation Device
NAT	Network Address Translation
NGN	Next Generation Network
NPS	Net Promoter Score
QoS	Quality of Service

RITM	Requested Item
SaaS	Software as a Service
SD WAN	Software Defined Wide Area Network
SOGEA	Single Order Generic Ethernet Access
SoW	Statement of Work
SSL	Secure Sockets Layer
URL	Uniform Resource Locators
WAN	Wide Area Network
VLAN	Virtual Local Area Network

10. Incident Classification and Operational Targets

Incidents affecting the operation of SD-WAN Managed Service are classified in accordance with the table below:

		Scale			
	Impact Description	**Business Wide**	**Department**	**Team**	**Individual**
Business Impact	Critical impact – It is not possible to complete key business tasks.	P1	P1	P2	P3
	High impact – Key business tasks are significantly degraded.	P1	P2	P3	P4
	Medium impact – The completion of key business tasks is made more difficult or is taking longer.	P2	P3	P4	P4
	Low impact – Service requests, incidents with no impact on business, or minor incidents where a workaround is available.	P3	P4	P4	P4

The associated response and resolution targets below will apply based on the incident priority assigned.

10.1 SD-WAN Operational Targets

We will endeavour to resolve SD-WAN incidents in line with the target resolution times below where you have procured our DIA or Managed WAN services. This excludes hardware replacement which is covered in section 5.7.

	P1	**P2**	**P3**	**P4**
Response	30 mins	1 hour	2 hours	4 hours
Fix (Resilient Access)	4 hours	8 hours	16 hours	40 hours
Fix (Protected Access)	6 hours	12 hours	24 hours	40 hours
Fix (Standard Access)	8 hours	12 hours	24 hours	40 hours
Fix (Standard Access-Broadband)	40 hours	40 hours	40 hours	40 hours
Fix (Management Platforms)	40 hours	40 hours	40 hours	40 hours
Hours of Support	24x7	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days	09:00 - 17:30, Business Days
Description	• For Resilient and Protected Access, total loss of both Primary Access Service and Secondary Access.	• For Resilient and Protected Access, total loss of either Primary Access or Secondary Access .	• Non-service affecting issue.	• Service Requests; • Non-Service affecting work and reports; or

	• For Standard Access, loss of Primary Access.	• For all access types, performance issues.		• A required change or configuration alteration to a service.

11. Service Levels and Service Credits

11.1 Service Levels

The service levels associated with this service are detailed below:

Service	Service Management Process	Metric	Target
Response	Incident management	Service desk response times	90% within the published response target
Fix	Incident management	Service desk fix times	90% within the published resolution target

11.2 Service Credits

The service credits associated with this service are detailed below:

Service	Tier	Measurement	Period	Target	Service Level	Service Credit
SD-WAN Standard MSDD	Essential	**Availability** - The ability to transmit a 64-byte IP data packet from the MSDD to the Designated Reference Router over the active Access Service and receive the response whilst not Congested.	Calendar Month	99.15%	98.49% - 98.4% Less than 98.4%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees
	Advanced		Calendar Month	99.9%	99.9% - 99.7% 99.69% - 99.3% 99.3% - 98.85% Less than 98.85%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees 20% of monthly value of Recurring Fees
SD-WAN Resilient MSDD	Essential		Calendar Month	99.9%	99.9 - 99.3% 99.3% - 98.85% Less than 98.85%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees
	Advanced		Calendar Month	99.99%	99.99% - 99.9% 99.29 - 98.85% 99.29% - 98.85% Less than 98.84%	5% of monthly value of Recurring Fees 10% of monthly value of Recurring Fees 15% of monthly value of Recurring Fees 20% of monthly value of Recurring Fees