SERVICE SCHEDULE G: ENTERPRISE MANAGED SERVICES (NON-DATA CENTRE)

THIS SERVICE SCHEDULE AND THE TERMS HEREIN APPLY TO THE SERVICES LISTED BELOW IF CUSTOMER HAS SUBSCRIBED FOR ONE OF THE TYPES OF THE SERVICES, IN ADDITION TO AND IN PREFERENCE OF THE GENERAL TERMS.

PART A – THE SERVICE

1. The Service

1.1 Types. Our Enterprise Managed Services comprise the following types that may only be subscribed by Customer if the Customer has firstly subscribed for the specified Qualifying Service prescribed in the table below. If more than one Qualifying Service exists for a Managed Service type, that Managed Service type is available to be subscribed to if the Customer has subscribed for either one of the Qualifying Services.

Nos.	Managed Service Type	Qualifying Service
(a)	Managed Perimeter Solution	Either Internet Direct or IPVPN
(b)	Managed WiFi	Internet Direct only
(c)	Wireless IPVPN	IPVPN only
(d)	Managed Router	Internet Direct, IPVPN, Eternet Voice
(e)	DDoS Protection/DDoS Shield/Advanced DDoS Shield	Internet Direct only
(f)	Managed Virtual Firewall	Internet Direct only
(g)	TIME Security Advanced Monitoring	Internet Direct, Data Centre Internet Access, Internet Protocol Virtual Private Networking or TIME Cloud Services
(h)	AVM Enforce Cloud Managed Services	AVM Cloud – Virtual Private Cloud (formerly known as Compute/Compute with database license)
(i)	IGS Enforce Managed Services 24 x 7 x 365	AVM Cloud – Virtual Private Cloud (formerly known as Compute/Compute with database license)
(j)	AVM Fusion Managed Services	AVM Cloud – Fusion Cloud (formerly known as AVM Cloud Fusion)
(k)	TIME WAF (Web Application Firewall): - TIME WAF (Standard Hosted Tenant) - TIME WAF (Standard) - TIME WAF (Premium)	Either Internet Direct or TCS.
(l)	Network Insight	IPVPN/Internet Direct/PLL with Managed Router
(m)	TIME Managed SD-WAN	Internet Direct (ID), PLL, FTTO

Nos.	Managed Service Type	Qualifying Service
(n)	TIME Secure DNS	Internet Direct, TCS. (This is also available for off-net Customers).
(o)	TIME Cloud Managed Service	TCS only
(p)	TIME PAM	TIME PAM (Privileged Access Management) - Standalone (core) product - VAS for Internet Direct, TIME Cloud Services and SDWAN
(q)	TIME MEN	TIME MEN (Managed Enterprise Network) - Standalone (core) product – packaged with ID, ID Lite, FTTO, ID/ID Lite Last Miles PLL (non-RFS site) and Fiber Broadband (non-RFS site)
(r)	TIME VA	TIME VA (Vulnerability Assessment) - Standalone (core) product
(s)	TIME MDR	TIME MDR (Managed Detection and Response) - Standalone (core) product
(t)	TIME Secure Network	Internet Direct
(u)	TIME Secure Network+	TIME Secure Network
(v)	TIME Network Analytics	Internet Direct, Managed SD-WAN, IPVPN, Managed Enterprise Network, Managed Router

(Each type shall hereinafter be referred to as ***"Managed Service"***)

1.2 Description. Each of the service types are described below.

No.	Managed Service Type	Detailed Service Description
(a)	Managed Perimeter Solution	Comprises of three (3) main services: (i) **Managed Security**: Dedicated physical firewall installed at the customer's premise together with TIME Internet Direct service. Only 2 brands offered under this package, Fortinet & Palo Alto. Other brands will be treated as a non-standard. All these are non-stock items and will only be ordered/purchased upon confirmed order from customer. (ii) **Managed Link Controller**: Dedicated physical Load Balancer installed at the customer's premise together with at least 2 lines of TIME Internet Direct service, or 1 line of TIME Internet Direct service and 1 other line from 3rd party Internet provider. Only 2 brands offered under this package, Peplink & F5. Other brands will be treated as a non-

No.	Managed Service Type	Detailed Service Description
		standard. All these are non-stock items and will only be ordered/purchased upon confirmed order from customer. (iii) **Managed WAN Optimiser**: Dedicated physical WAN Optimiser installed at the customer's premise that goes together with TIME Internet Direct service, to optimise the bandwidth usage. Only 2 brands offered under this package, Silverpeak & Riverbed. Other brands will be treated as a non-standard. All these are non-stock items and will only be ordered/purchased upon confirmed order from customer. Additional information in the downloadable factsheet is available at http://www.time.com.my/enterprise/managed-services/security-and-performance-optimisation
(b)	Managed WiFi	This service is a private wireless network for employees, as well as public WiFi network for guests in one fully managed, end-to-end solution. It is a secure and reliable connectivity option suitable for small sites, branches, large facilities, campuses or distributed multi-site businesses. The solution comes with the following Managed Services Equipment ("MSE") i.e. router, switches, Access Points, Internet Access Management, which are installed at customer's premise. All MSE are non-stock item and will only be ordered/purchased upon confirmed order. The procurement, installation, set up and configuration of the MSE is done by TIME, including periodic monitoring. It removes the burden from the Customer to manage and monitor its WiFi network, allowing it to concentrate its human capital on other matters.
(c)	Wireless IPVPN	This is a wireless IPVPN service that uses the 3G/4G network belonging to third party providers. This solution is complementary to TIME's IPVPN service. It is suitable for machine to machine applications (e.g. ATMs), non-critical application, SCADA, POS or last mile access at non-RFS areas. This solution offers 2 options; Single SIM & Dual SIM: (i) **Single SIM -** Using Celcom SIM card at 5GB quota as a standard. Recommended deployments are: for non-critical data traffic usage or as a backup for the TIME's fixed line. (ii) **Dual SIM** - Combination of Celcom & Maxis SIM card and both are at 5GB quota as a standard. Recommended deployments of a dual SIM are for redundancy purpose via different Mobile Operator or where customer may require a service level availability of 99.5%.
(d)	Managed Router	Router functions that is offered on top of Internet Direct or IPVPN subscription. It comes with two (2) options: (i) **Physical Router** - Dedicated physical router installed at the customer's premise. Two (2) options offered to the customers; standard & non-standard routers: • **Standard Router** - Stock item that is stored at TDC warehouse and it is readily available. The stocked router models Cisco 4321, 4331, C8200L-1N-4T, C8300-1N1S-6T and Fortinet FG-80F & FG-100F.

No.	Managed Service Type	Detailed Service Description
		• **Non-Standard Router** - Non-Stock item that is only ordered/purchased upon confirmed order. The model types are Cisco 4351, 4431, 4451, and any other router models preferred by the customer. (Eternet Voice comes with physical router option only) (ii) **Virtual Router** – Delivering the network service such as routing and virtual private network connectivity to customer by using software rather than physical hardware.
(e)	DDoS Protection/DDoS Shield/Advanced DDoS Shield	This is a fully on-network DDoS protection system that resides within the TIME Network or customer premises (for application attack) and comprises a set of techniques and/or tools for resisting or mitigating the impact of distributed denial-of-service (DDoS) attacks on networks attached or connected to the Internet by protecting the target and relay networks. The service enables detection to be undertaken, diversion of suspected attack away from the target, filtering DDoS traffic from legitimate traffic and analysis of the traffic and log files. On-premise physical hardware may or may not be required for this solution. This Managed Service type addresses volumetric and application attacks to the customer's network or systems.
(f)	Managed Virtual Firewall	Managed Virtual Firewall is a secure virtual network function (VNF) that handles all the capabilities of a traditional, premises-based firewall hosted on a dedicated hardware, without the need for any physical hardware to be installed at customer's premises. This Managed Service type is a virtual firewall system that is hosted within TIME's Network, and only requires an appropriate system set up at the TIME Network that will be undertaken by TIME. There is no on-premise physical hardware that is required for this Managed Service type. This Managed Service addresses specific packet attacks to the customer's network or systems and not volumetric attacks.
(g)	TIME Security Advanced Monitoring	TIME Security Advanced Monitoring (TSAM) is a remote solution that involves an information security team in TIME who monitors and analyses an organisation's consolidated security system on an ongoing basis. TSAM runs on a Security Incident and Event Management system offered as a hosted service.
(h)	AVM Enforce Cloud Managed Services	Comprises the following services: (i) **DR Recovery Shared Office Space @ Cyberjaya** – The service is to provide a work area solution for disaster recovery purposes where seat(s) are assigned within a shared office suite. It is located at Cyberjaya. (ii) **Managed Backup and DR Only** – Managed backup service is to manage the data backup platform of the Qualifying Service that is able to carry out data backup for

No.	Managed Service Type	Detailed Service Description
		the Customer and includes the Standard Service Scope only. Managed DR service is to manage replication of customer's data to another zone and also to provide data availability in the event of site failure. (iii) **Managed Cyber Security** – This service is to provide Security Information and Event Management (SIEM) for each of the security devices in the Customer's cloud environment. The Customer will receive monthly reports in relation to SIEM service. (iv) **Managed Firewall** – This service is to manage the firewall system for the Qualifying Service. (v) **Managed OS, Patching, Backup and DR** – This service is to manage the centralised data backup platform of the Qualifying Service that is able to carry out data backup for the Customer and includes the Standard Service Scope. It also includes the provision by TIME of an operating system licensed software and/or database licensed software.
(i)	IGS Enforce Managed Services 24 x 7 x 365	**Managed Services 24 x 7 x 365** – This service is to provide outsourcing service to the Customer to conduct on-site operation, and anticipating the Customer's need for, a range of processes and functions in order to improve the operations.
(j)	AVM Fusion Cloud Managed Service	**Fusion Managed Service** – This service is to manage the cloud backup and replication platform of the specific Qualifying Service to which this service is applicable, that is able to carry out data backup and replication for the Customer and includes the Standard Service Scope only.
(k)	TIME WAF (Web Application Firewall): - TIME WAF (Standard Hosted Tenant) - TIME WAF (Standard) - TIME WAF (Premium)	TIME WAF (Web Application Firewall) – This service is to provide managed Web Application Firewall (WAF) to the Customer. It comes in three (3) package offerings: (i) **TIME WAF (Standard Hosted Tenant)** – This service is a shared virtual WAF that is hosted within TIME's Network with multi-tenant set up for the separation of customers' profile. (ii) **TIME WAF (Standard)** – This service comes with two (2) options: • **Hosted (Dedicated)** – This service is a dedicated virtual WAF hosted within TIME's Network, with dedicated set up for the Customer. • **On-Premise** – This service is a WAF service with dedicated hardware installed at the Customer's premise. (iii) **TIME WAF (Premium)** – This service is the TIME WAF (Standard) service with additional advanced features namely, sandbox cloud service and credential stuffing defense service.
(l)	Network Insight	Network Insight Services is a value added service to IPVPN, Internet Direct and PLL that will provide insights to enterprises network. Insights are based on the following parameters on real time and historical data:

No.	Managed Service Type	Detailed Service Description
		(i) Managed Routers Utilisation (CPU, Memory and Temperature). (ii) Managed Routers Uptime. (iii) Netflow Reporting.
(m)	TIME Managed SD-WAN	TIME Managed SD-WAN comes in 3 offerings - SD-WAN Premier, Basic and Lite: (i) SD-WAN Premier is a hybrid connectivity service leveraging on PLL and ID access for customer with critical business site, require high bandwidth, backup and high SLA. (ii) SD-WAN Basic is purely public connectivity service leveraging on ID and FTTO access for customer with critical business site, require backup and high SLA. (iii) SD-WAN Lite is purely public connectivity service leveraging FTTO access. It caters to non-critical business site by providing best effort SLA via 100Mbps FTTO.
(n)	TIME Secure DNS	This service is to provide the secure domain name hosting of Customer's domain name.
(o)	TIME Cloud Managed Service	This service is to provide the managed services for the TIME Cloud Services, it comes in 4 type managed services as below: (i) Managed Operating system - This service oversees, maintains, and optimizes an organization's operating system, handling tasks like updates, troubleshooting, and OS performance management for an up-to-date environment (ii) Managed Backup and Restore - Managed backup and restoration of critical data and systems, ensuring data integrity and providing a reliable recovery solution in case of data loss, system failures, or disasters. (iii) Managed Patching - This service offers semi-annual patching, accompanied by Windows Update Reports for Customer awareness. To enhance security, VMs are snapshotted pre-patching and post-patching VM statuses are closely monitored. This streamlined process prioritizes security, transparency, and quick recovery. (iv) Managed DR - This service encompasses the configuration and management of disaster recovery activities, featuring cross-zone replication, real-time monitoring of replication status, and expert assistance during failovers and fall-backs.
(p)	TIME PAM	This service is to provide Privileged Access Management in 2 packages as below; (i) TIME PAM – Designed for small to medium size enterprise (ii) TIME PAM Pro – Design for medium to large enterprise The purpose of PAM is to ensure the privileged access to an important asset is resecured as well as for audit trail purposes.

No.	Managed Service Type	Detailed Service Description
		The PAM System will enforce the strong access authentication with multi-factor authentication (MFA) and the objective is to identity security solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources.
(q)	TIME MEN	This service is to provide comprehensive Managed Enterprise Network as below; (i) Internet Access (ii) Internet Router (iii) WAN Security (Firewall) (iv) Local Area Network (v) Wireless Access (vi) Related Value-Added Services SDWAN is also available for selected technology platform to fulfil the end-to-end network services requirement by enterprise entity.
(r)	TIME VA	The Vulnerability Assessment (VA) service, powered by Tenable.SC, is the assessment to identify the security weakness (vulnerability) in the information system infrastructure. The service is offered within minimum 1 year contract (4 x quarterly scanning) with the report and advisory by TIME Cybersecurity Team.
(s)	TIME MDR	TIME Managed Detection and Response (MDR) is a remote solution that involves a cybersecurity team in TIME who monitors, detects, analyses and responds to an organisation's consolidated security system on a 24x7 basis. It has the capability of detection of threats at a lateral level (across cloud, networks and endpoint): (i) Holistic monitoring and detection (ii) Consolidation of events and targeted response (if required) TIME MDR runs on open MDR platforms offered as a hosted service.
(t)	TIME Network Analytics	TIME Network Analytics is a PRTG-based network monitoring and analytics service that extends visibility from TIME's connectivity links to customer edge devices. The service provides: • The service enables the Customer to monitor network performance through a self-service web dashboard, providing both real-time and historical performance data, • Combined with TIME's proactive Severity 1 alarm monitoring and customer notification

No.	Managed Service Type	Detailed Service Description
		The Standard Package comprises five (5) sensors per device, covering the following key metrics: • WAN uptime • Latency, jitter and packet loss; • Application reporting • Device health - CPU utilisation • Device Health - memory utilisation. Additional sensors may be provisioned as add-on services, subject to scope evaluation and feasibility assessment by TIME

1.3 Scope of Service

1.3.1 **Overall Scope of Work.** Each of the Managed Service types comprises a Standard Service Scope as detailed below.

Nos.	Managed Service Type	The scope of work for each type of the Managed Service that TIME will provide is specified below (***"Standard Service Scope"***)
(a)	Managed Perimeter Solution	(i) Order, supply and deliver the MSE; (ii) Install and configure the appropriate MSE; (iii) Reset the appropriate MSE when malfunctions; (iv) Carry out the appropriate MSE configuration backup; (v) Update firmware and vulnerability patches of the appropriate MSE; (vi) Replace any damage or malfunctioning MSE (according to Paragraph 4.4.1 of this Service Schedule); (vii) Router change management / modification & documentation; (viii) Advance configuration of the appropriate MSE (where applicable); and (ix) Uptime monitoring.
(b)	Managed WiFi	(i) Supply and deliver enterprise grade WiFi router; (ii) Install and configure the WiFi routers supplied; (iii) Carry out a site survey of the Service Location before implementation; (iv) Internal cabling installation; (v) Reset router, access point or bandwidth management when such MSE malfunctions; (vi) Carry out applicable MSE configuration backup; (vii) Update firmware and vulnerability patches of the Router, access point or bandwidth management appliances; (viii) Replace any damage or malfunctioning Router, access point or bandwidth management (according to Paragraph 4.4.1 of this Service Schedule); (ix) Router, access point or bandwidth management change management / modification & documentation; (x) Advance Router, access point or bandwidth management configuration (where applicable); (xi) Uptime monitoring; and (xii) Resolve connectivity issues if it pertains to Internet access.

(c)	Wireless IPVPN	(i) Carry out and provide the solution design following Customer request and requirements; (ii) Appoint personnel with regards to the planning and preparation of this Managed Service type; (iii) Review the Customer's existing network environment and identify, with the Customer, the Customer's desired key locations to deploy this Managed Service type; (iv) Conduct an environment study on how the tools shall be suitably placed and implemented; (v) Procure from wireless network provider the appropriate 3G or 4G SIM card; (vi) Order, procure and deliver the applicable MSE; (vii) Carry out installation of MSE according to Customer's network infrastructure; (viii) Configure the MSE including installing the SIM card; (ix) Commission the MSE, SIM card and the Managed Service; (x) Carry out a user acceptance test before going live; (xi) Fine-tuning the applicable MSE as and when required; (xii) Provide deployment documentation once the Managed Service has commenced; (xiii) Carry out one (1) project handover training and one (1) project briefing to Customer's selected personnel (which shall not be more than 10 persons); (xiv) Reset the router when it malfunctions; (xv) Carry out periodic router configuration backup; (xvi) Update firmware and vulnerability patches of the router; (xvii) Replace any damage or malfunctioning MSE (according to Paragraph 4.4.1 of this Service Schedule); (xviii) Router change management / modification & documentation; (xix) Advance router configuration; (xx) Uptime monitoring; and (xxi) Support management comprising Real-time network visibility, End-to-end service fault rectification, Prioritised support and In-depth reporting.
(d)	Managed Router	For physical router: (i) Order, procure, supply and deliver the applicable MSE; (ii) Install and configure the applicable MSE; (iii) Reset the MSE when it malfunctions; (iv) Carry out the configuration backup of the applicable MSE; (v) Update firmware and vulnerability patches of the applicable MSE; (vi) Replace any damage or malfunctioning MSE (according to Paragraph 4.4.1 of this Service Schedule); (vii) Router change management / modification & documentation; (viii) Advance router configuration; and (ix) Uptime monitoring. For virtual router: (i) Configure the virtual router; (ii) Reset the virtual router when it malfunctions; (iii) Restore the virtual router as quickly as possible; (iv) Carry out virtual router configuration back up; and (v) Uptime monitoring.

(e)	DDoS Protection/DDoS Shield/Advanced DDoS Shield	This Managed Service type is a DDoS protection system that is hosted within TIME's Network, and only requires appropriate system set up at the TIME Network that will be undertaken by TIME. On-premise physical hardware may or may not be required for this Managed Service type. Enable network reporting which comprises: (i) Provision of access to a customer web portal, real time network visibility (even during attacks), access to historical records; (ii) Incident reporting from TIME to customer; (iii) Attack notifications from TIME to customer; (iv) Undertake performance support which comprises providing a dedicated account manager, certified technical teams and 24 x 7 x 365 days/year proactive network monitoring; (v) Performing non-intrusive packet inspection; and (vi) Performing automatic intervention and counter measure execution.
(f)	Managed Virtual Firewall	(i) Configure the virtual firewall; (ii) Reset the virtual firewall when malfunctions; (iii) Restore the virtual firewall as quickly as possible; (iv) Carry out configuration backup of the virtual firewall customer settings; (v) Update firmware and vulnerability patches (where applicable); (vi) Advance configuration of the virtual firewall (where applicable); (vii) Define malicious traffic to be blocked; (viii) Uptime monitoring; (ix) Undertake performance support which comprises providing a dedicated account manager, certified technical teams and 24 x 7 x 365 days/year proactive network monitoring; (x) Performing non-intrusive packet inspection; and (xi) Incident reporting from TIME to customer.
(g)	TIME Security Advanced Monitoring	TSAM's scope comprise the following components: (i) Network security monitoring; (ii) Network security threat detection; (iii) Network security log analysis; (iv) Incident response notification; and (v) Network security reporting. TIME will provide the TSAM: (i) Via centralised platform and the public or private network; and (ii) Through a method between the Customer's equipment and TIME's equipment that TIME will confirm to the Customer upon request.

		Each element of the TSAM Services comprises one or more stages, depending on the service: (i) the first stage is provided on a one-off basis at the start of your service; (ii) the second stage is provided on an ongoing basis during the term, once the first stage is completed; and (iii) the third stage is provided periodically during the term as TIME deems necessary. Detailed information is available at https://www.time.com.my/enterprise/security/security-monitoring
(h)	AVM Enforce Cloud Managed Services	AVM Enforce Cloud Managed Services scope comprise the following: (i) Technical support on a per-incident basis; (ii) Where applicable, remote or on-site technical support on error and technical product problems; (iii) Provision of analysis log when the incident is logged; (iv) Performing diagnostic test using in-built tools, if applicable (v) 24 x 7 x 365 technical team on standby; (vi) Provision of basic guide on software operation; (vii) Where applicable, assistance to verify the software patching on the environment before upgrade (excluding the performance of the patching activity); (viii) Provision of Incident Report for all Severity Level 1 Qualifying Incidents; (ix) For the DR Recovery Shared Office Space @ Cyberjaya service, provision of shared disaster recovery seat with shared facilities.
(i)	IGS Enforce Managed Services 24 x 7 x 365	IGS Enforce Managed Services 24 x 7 x 365's scope comprises the following: (i) Provide technical support on a per-incident basis; (ii) Where applicable, provision of remote or on-site technical support on error and technical product problems; (iii) Provision of analysis log when the incident is logged; (iv) Performing diagnostic test using in-built tools, if applicable (v) 24 x 7 x 365 technical team on standby; (vi) Provision of basic guide on software operation; (vii) Where applicable, assistance to verify the software patching on the environment before upgrade (excluding the performance of the patching activity); and (viii) Provision of Incident Report for all Severity Level 1 Qualifying Incidents.
(j)	AVM Fusion Cloud Managed Service	(i) Provide initial backup storage volumes and additional backup storage volumes as required by the Customer; (ii) Provisioning of initial configuration of backup policy; (iii) Provisioning of backup policy modification and/or optimisation; (iv) Provide proactive monitoring of backup success or failure; (v) Creation of backup reports; (vi) Provisioning of restoration of backups as required by the Customer;

		(vii) Verification of successful backup; (viii) Provide notification of successful restoration of backups; (ix) Provide notification of storage volume threshold being exceeded; (x) Provide notification of backup anomalies or issues; (xi) Provide administration of backup services; (xii) Create, delete or modify the login credentials of the Customer's backup users; (xiii) Troubleshooting of the backup and/or restoration job failure; (xiv) Restoring the backup to cloud compute infrastructure; and (xv) Provisioning of backup policy enforcement.
(k)	TIME WAF (Web Application Firewall): - TIME WAF (Standard Hosted Tenant) - TIME WAF (Standard) - TIME WAF (Premium)	(i) Deliver and manage the TIME WAF as a Managed Service; (ii) Respond and manage any incidents related to service availability; (iii) Ensure the web application firewall is running on stable firmware version as per recommendation by manufacturers of the web application firewall; (iv) Provide protection to Customer's web application as per subscribed package; and (v) Provide support to Customer for change management of the web application firewall rules based on product specification under the Customer's subscribed package for up to ten (10) times a year. For clarity, every such change management request exceeding ten (10) times a year will be subject to additional charges to the Customer.
(l)	Network Insight	(i) Order, configure, monitor, troubleshoot, rectify fault reported by customer. (ii) Provide access to Self Care portal and ensuring Self Care uptime. (iii) Update firmware and vulnerability patches of the applicable MSE.
(m)	TIME Managed SD-WAN	The items mentioned below are the standard component for SD-WAN: (i) SD-WAN router – will be installed inside a single location at customer premises. (ii) SD-WAN Cloud Controller – hosted at TIME data centre; (iii) Connectivity – via PLL, ID or FTTO access. The items mentioned below are the standard scope of work for SD-WAN: (i) Providing Connectivity via PLL, ID or FTTO and ensuring its uptime. (ii) Self-serve reporting of the SD-WAN links on historical and real time basis via Self Care portal and ensuring its uptime (iii) Order, configure, monitor, troubleshoot, rectify fault reported by customer. (iv) Maintain and monitor health of the SD-WAN Cloud Controller hosted at TIME data centre.
(n)	TIME Secure DNS	(i) Deliver and manage the secure DNS for the Customer's hosted domain.

		(ii) Ensure the secure DNS is up and running in functional condition as per SLA.
(o)	TIME Cloud Managed Service	(i) Managed Operating system: - Assist OS installation/provision. ● Monitoring Virtual Machine Performance/disk usage and alert Customer when abnormal. - Assist troubleshooting when any issue relates to OS but exclude application related issue. ● Example: Operating system error after patching. - Generate the report for virtual machine performance report. - Generate the compute usage report. - Assist Network configuration (IP configuration). - TIME required local administrator right to perform manage OS task. - Administration responsibility is sharing between Customer and TIME Support. - TIME only performs changes based on request. - Any operating system is EOL (End of Life) only provide best effort. (ii) Managed Backup and Restore: - Configure and managed backup. - Backup policy modification, optimization and best practices. - Monitor backup job and provide daily backup status. - Monitor backup capacity usage and provide monthly usage report. - Assist to perform any restoration from the backup when request. - Troubleshoot any backup related issue. - Provide best effort troubleshooting on application related issue after performed restoration. - TIME only performs changes based on request. (iii) Managed Patching: - Half-yearly patching. - Windows Update Report to Customer. - Snapshot the VM before patching and keep for 3 days. - Follow up VM status after patching. (iv) Managed DR: - Configure and managed DR activity include below: ● Cross zone replication. ● Monitoring replication status. ● Assist to failover and fall-back when DR activity. ● Provide DR activity report. ● By default, will have 10 days DR activation per year. - TIME only performs DR based on request.
(p)	TIME PAM	(i) Provide licensed access to Privileged Access Management (PAM) which is hosted in TIME Cloud; (ii) Provide licensed access to the PAM platform, which will be multi-tenanted, with each Customer as a tenant having their own dedicated administrative access;

		(iii) Ensure the PAM platform is running on a stable firmware version as recommended by the PAM platform principal or provider; and (iv) Provide the necessary support to the Customer as Managed Services within the scope of PAM Services.
(q)	TIME MEN	(i) Delivery of the related hardware and virtual system, including licenses, as specified in the Service Order; (ii) Provide the following items: a) Internet Access; b) Internet Router; c) WAN Security (Firewall); d) Local Area Network; e) Wireless Access; f) Related Value-Added Services as specified in the Service Order; (iii) Ensure the related system is running on a stable firmware version as recommended by the hardware manufacturers and the system provider or principal; and (iv) Provide the necessary support to customer as Managed Services within the scope of MEN Services.
(r)	TIME VA	(i) Plan and prepare for the VA scanning, subject to the Customer providing the requested information to TIME, including but not limited to technical requirements; (ii) Conduct VA scanning as subscribed by the Customer; (iii) Generate VA scanning reports; (iv) Provide advisory as per the VA scanning report; no advisory will be provided for the same result of previous VA scanning; and (v) Recovery from the identified vulnerability is out of the scope of the VA Services.
(s)	TIME MDR	TIME MDR's scope comprise the following components: (i) Network security monitoring; (ii) Network security threat detection; (iii) Network security log analysis; (iv) Incident response notification; and (v) Network security reporting. TIME will provide the MDR: (i) Via centralised platform (which may be a public or private network); and (ii) Through a method between the Customer's equipment and TIME's equipment which TIME will confirm to the Customer, upon Customer's request. Detailed information is available at https://www.time.com.my/enterprise/security/security-monitoring
(t)	TIME Secure Network	**Description of Service**

		(i) TIME Secure Network is a network-based threat communication visibility service made available to Customers subscribing to Internet Direct. (ii) The service is formed and delivered based on the fixed public IP address assigned by TIME to the Customer under the subscribed Internet Direct service. (iii) Using NetFlow sample generated within TIME's network, TIME correlates traffic associated with the Customer's assigned fixed public IP address against threat intelligence databases. (iv) TIME provides the Customer with secure login credentials to access a web-based dashboard hosted by TIME. (v) The dashboard displays detected suspicious or malicious communications associated with the Customer's assigned fixed public IP address, including but not limited to: - Source and destination IP addresse - Date and time of detected communication - Traffic direction (inbound or outbound) - Threat classification - Volume and frequency of detected communication events - Historical event logs within the applicable data retention period (vi) TIME does not block, filter, modify, inspect payload content or otherwise interfere with Customer traffic. (vii) The service provides visibility of detected threat communications only and does not include traffic blocking, remediation, incident response, forensic investigation, endpoint analysis or active prevention capabilities. (viii) Enforcement or blocking capabilities, if required, are available separately under TIME Secure Network+ (subject to subscription).
(u)	TIME Secure Network +	**Description of Service** (i) TIME Secure Network+ is an inline network threat enforcement service that may only be subscribed to by Customers with an active TIME Secure Network and Internet Direct service. (ii) The service is deployed within the Customer's network environment, positioned inline between the Internet Direct termination point and the Customer's firewall infrastructure. (iii) The service is provisioned using a physical DarkShield security appliance, supporting up to a 1Gbps interface per subscribed instance.

		(iv) All Internet-bound and/or inbound traffic intended for inspection must traverse the DarkShield appliance for enforcement. (v) The appliance performs real-time inspection and correlation of traffic against threat intelligence databases and predefined enforcement policies. (vi) Upon detection of confirmed malicious communication, the service may automatically: - Block or drop traffic associated with known malicious IP addresses or domains; - Prevent outbound communication to identified command-and-control (C2) infrastructure; - Enforce policy-based traffic restrictions based on configured threat categories. (vii) TIME Secure Network+ includes dashboard visibility (as provided under TIME Secure Network) of detected threats and enforcement actions taken. (viii) Enforcement capability is limited to traffic that passes through the deployed DarkShield appliance and is subject to interface capacity limitations of up to 1Gbps per subscribed instance. (ix) TIME Secure Network+ does not include endpoint protection, internal east-west traffic monitoring, application-layer forensic investigation, vulnerability remediation, or guaranteed prevention of all cyber threats. (x) TIME does not guarantee absolute protection against all malicious traffic or security incidents. The service operates on a best-effort basis within the technical constraints of the deployed DarkShield platform and Customer network configuration.
(v)	TIME Network Analytics	**Description of Service** (i) Provision and configure the TIME Network Analytics platform, including deployment of sensor and setup of the monitoring dashboardfor the subscribed device(s); (ii) Configure alarm thresholds and dashboard maps customised to the Customer's environment; (iii) Provide the Customer with access to a self-serve web-based Network Analytics Dashboard for real-time and historical network performance monitoring; (iv) Provide alert-to-action guidance indicating the nature of the alarm, recommended preliminary checks, and escalation accountability for severity 1

		(v)	Maintain and ensure availability of the Network Analytics platform hosted on TIME Cloud and
		(vi)	Provide self-service reporting, with monthly reporting available where a Service Manager is assigned.

(For the purposes of this Service Schedule, the words **"MSE"** or **"Managed Service Equipment"** means the particular equipment to be provided by TIME as part of the type of Managed Service subscribed and installed at the Service Location).

1.3.2 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that the MSE will not malfunction, is fit for purpose and is of merchantable quality, whether stand alone, in combination with any Customer Equipment or other equipment and software.

1.4 During the Initial Service Term (and any Renewed, TIME will provide to Customer, and Customer will obtain from TIME, the Managed Service as subscribed by the Customer in the applicable Service Order or the agreed quotation (as the case may be).

1.5 Quotation & Subscription.

1.5.1 If you intend to subscribe for any of the above Managed Service types, TIME will provide you a quotation specifying the details of the type of Managed Service containing the MRC payable, the quantity of MSE to be supplied and installed, the minimum contract period, and such other relevant information as may be required.

1.5.2 If the quotation issued by TIME is acceptable to you, you will sign and return a duplicate of the quotation or signify your acceptance in such written form as may be acceptable to TIME. Only upon your acceptance of the quotation, and subject to Clause 3.2 General Terms, TIME will provision the Managed Service.

1.5.3 **Non-Standard Service Scope.** If the scope of work for a Managed Service type is not the Standard Service Scope, then the following conditions apply:

(a) If TIME has provided a quotation to the Customer which specifies a scope of work different from the Standard Service Scope, and the quotation is accepted by the Customer, then such scope of work shall be the scope of work to be undertaken and performed by TIME, notwithstanding anything to the contrary herein.

(b) TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that the Managed Service will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality.

(c) Such other terms and conditions as may be specified and agreed in an agreed letter of award from the Customer to TIME.

2. SERVICE COMMENCEMENT & CANCELLATION

2.1 Service Commencement

2.1.1 The Managed Service shall commence on the same SCD as the Qualifying Service.

2.1.2 If the Managed Service subscribed is to commence on a CRD (which is after the SCD of the Qualifying Service), the Managed Service will commence on such date as may be

notified by TIME in writing, and the Initial Service Term of the Qualifying Service will be automatically extended so that the expiry date of the Managed Service and the Qualifying Service are the same.

2.1.3 TIME shall complete the installation works of the MSE by the CRD unless TIME experiences delays due to causes beyond its control, Force Majeure Event, or acts or omissions of third party suppliers. If TIME is of the opinion that the CRD may not be achieved TIME may revised the CRD and notify the Customer accordingly.

2.2 Service Cancellation by Customer

2.2.1 Where the Customer cancels and/or wishes to cancel the Service Order partly or wholly at any TIME prior to the SCD for any reason whatsoever, the Customer shall be liable to pay the Cancellation Charges as set in Paragraph 11.3.

2.3 Service Cancellation by TIME

2.3.1 If the Customer delays or fails to perform any of its obligations in this Service Schedule, including Paragraph 3.1, before the CRD, then at TIME's option, TIME may upon notice to the Customer, either:

(a) change the CRD;
(b) cancel the relevant Service Order(s) and the Customer shall pay the Cancellation Costs as invoiced by TIME; or
(c) invoice the Customer for any reasonable charges incurred for any work that is performed by TIME on behalf of the Customer and that is directly attributable to the Customer's failure or delay to perform where such work is necessary to provide the Services, and Customer is to pay such an invoice within fourteen (14) days from the date of receipt of this invoice. A failure to do so may result in the Service not being commissioned by TIME by the CRD.

2.3.2 TIME may, in addition to any other Paragraph in this Service Schedule, cancel a Service Order for the Managed Service identified in this Service Schedule if it is technically not feasible to provide the Service by the CRD or if third party providers are required, such third party providers are not able to provide their element of the Managed Service, and accordingly neither Party is liable to the other for any loss, costs or expense, and no Balance Charges, Termination Charges and/or Cancellation Costs are payable by Customer.

3. SERVICE LOCATIONS

3.1 Customer's Obligations at Service Locations

3.1.1 The Customer will at its own expense and prior to the CRD and in advance of any installation work by TIME:

(a) ensure that all information, items or consents as may be either requested by TIME or required in order for TIME to supply and install the MSE or provision the Managed Service, are made available or obtained at the Customer's own cost in sufficient TIME to enable the CRD or any revised CRD to be achieved;
(b) obtain all necessary consents, including consents for any necessary alterations to buildings and any consents required for the installation, use and maintenance of any MSE at the Service Locations for the Term;
(c) provide, prepare and maintain the specific points, locations or spaces as required by TIME within the Service Locations for the installation of the MSE;
(d) provide a secure, continuous and appropriate electrical power supplies (AC or DC supply) for the operation and maintenance of the MSE at such points and with such

connections as TIME specifies, including necessary electrical points required by TIME in order to provide the Managed Service;

(e) UNLESS OTHERWISE AGREED, in order to mitigate any Service interruption resulting from failure in the principal power supply, provide back-up power with sufficient capacity to conform to the standby requirements of the applicable standards;

(f) provide a suitable and safe working and operational environment and notify TIME of any health and safety rules and regulations and security requirements that apply at the Service Location;

(g) provide all necessary trunking, conduits, cable trays and mounting points as may be required;

(h) provide internal cabling between the MSE and any Customer Equipment, as appropriate, unless Paragraph 1.3.2 of this Service Schedule specifies otherwise;

(i) take up or remove any fitted or fixed floor coverings, ceiling tiles and partition covers in TIME to allow TIME to undertake any necessary installation, provisioning or maintenance of the MSE and/or the Managed Service;

(j) ensure that any floor loading limits will not be exceeded;

(k) carry out any work that may be required after installation, provisioning or maintenance work is completed to make good any cosmetic damage caused during the installation, provisioning or maintenance of the Managed Service; and

(l) Customer grants TIME or shall procure or assist in the procurement of rights for TIME to install, place and affix the MSE at the designated areas in the Service Locations until the expiry of the Term.

3.1.2 If TIME must change a Managed Service due to incomplete or inaccurate information provided by the Customer, TIME may, charge the Customer such additional charges that may be reasonably incurred for carrying out such a change.

3.1.3 The Customer will comply with TIME's reasonable requests that are necessary for reasons of health and safety, environment, sustainability, security or quality or performance of the Managed Services.

3.1.4 **Right of Entry ("RoE").**

(a) **Prior Notification.** Upon reasonable notice from TIME, and unless (b) below applies, the Customer grants the requisite Permissions that are reasonably necessary for TIME and TIME Team to enter, remain upon or exit the Service Location at all reasonable TIMEs to install, provision or maintain the MSE or Managed Service including set up, deliver and maintain the Managed Service, recover or remove any MSE and perform its obligations under this Service Schedule.

(b) **Customer to obtain 3rd Party RoE.** Customer shall promptly obtain the necessary third party Permissions from the landlord, building manager or joint management board (as applicable to a Service Location) for TIME and TIME Team to Use the Service Location, and such Permission shall subsist until expiry of the Term, at no charge to TIME. Customer is to provide TIME with a copy of such Permission as soon as it receives the same.

3.2 Use of Service Location: TIME may Use the Service Location, at no charge to TIME, until the expiry of the Term. If TIME's Use of the Service Location is subject to any charges by any third party, such charges shall be reimbursed by Customer and included in all invoices from TIME to Customer.

3.3 Vacating Premises. If the Customer intends to vacate the Service Location, the Customer is to notify TIME at least six (6) months prior to vacating the Service Location, in order that TIME may prepare for the orderly cessation of the Managed Service.

3.4 **Managed Services only at Service Location.** The Managed Services will only be provided by TIME at the specific Service Locations identified in the quotation or Service Order (as the case may be) and not any other location belonging to, under the control of or being used by the Customer.

4. MSE – TITLE, SUPPLY & WARRANTY

4.1 The legal and beneficial title in the MSE supplied in respect of or as part of the subscribed Managed Service, subject to Paragraphs 4.2 and 4.3 below, shall belong to and remain with TIME, notwithstanding the delivery, installation and provisioning of any MSE at Service Locations.

4.2 TIME may transfer the legal and beneficial title to the Customer on the expiry of the Term PROVIDED ALWAYS THAT all sums due and/or owing (including the Charges, and where applicable, Cancellation Costs or Termination Charges (if any) and the Balance Charges) are paid by the Customer in their entirety.

4.3 Quantity & Defects

4.3.1 If the quantity of MSE supplied is less than the quantity prescribed in the quotation, Customer will not reject the supply nor cancel the Service Order, but TIME will deliver the balance quantity as soon as reasonable practicable at no additional cost to the Customer, and the CRD may be extended by TIME if necessary.

4.3.2 The Customer shall not reject any of the MSE delivered, except if the packaging of the MSE is visibly damaged at the point of TIME of delivery to the Service Location, whereupon TIME may procure and deliver replacement MSE at no additional costs to Customer.

4.3.3 If after delivery of the MSE but before the SCD, any MSE is found to be defective or damaged, then such damaged or defective MSE shall be replaced by TIME at no additional cost to Customer PROVIDED ALWAYS THAT such damage or defect is not caused by the Customer, its servants or agents or any third party, whilst the MSE is in the Customer's custody, possession or control.

4.4 Defects after SCD

4.4.1 If after the SCD and throughout the Initial Service Term only, if any MSE is found to be defective, damaged or have malfunctioned, the Customer shall notify TIME of the same, and such MSE shall be replaced as soon as reasonably practicable by TIME and at no additional cost to Customer, unless such defect, damage or malfunctioning is caused or contributed by the Customer's, their servants', agents', invitees' or third party's acts or omissions (including negligent acts or omissions).

4.4.2 The warranty hereby granted shall cease upon the expiry date of the Initial Service Term and for the avoidance of doubt, shall no longer be applicable during the Renewed Service Term.

5. SERVICE TERM.

5.1 **Initial Service Term.** Unless otherwise prescribed in Paragraph 6 herein in respect of a type of Managed Service or in the quotation issued by TIME and accepted by Customer, and notwithstanding anything to the contrary in the General Terms, the Initial Service Term is for a period of twelve (12) months commencing from the SCD as specified in a notice issued by TIME.

5.2 **Renewed Service Term.** Unless Customer notifies TIME in writing at least 90 days before the expiry of the Initial Service Term, that the Initial Service Term is not to be renewed, the Service shall be automatically renewed for the same duration as the Initial Service Term, on the same General Terms and the terms in this Service Schedule.

6. SPECIAL CONDITIONS FOR SPECIFIC SERVICE TYPES

Notwithstanding anything to the contrary in the General Terms or elsewhere in this Service Schedule, if the Managed Service is:

6.1 Managed Perimeter Solution Service type. If the Managed Service type subscribed is Managed Perimeter Solution, the following conditions shall apply.

6.1.1 Should Customer require TIME to carry out any additional work beyond the Standard Service Scope, TIME may do so and charge the Customer a fee for such additional work. Prior to executing the additional work requested, TIME will provide a quotation and if the Customer agrees such quotation will vary this Agreement.

6.1.2 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that the Managed Service will perform to the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality.

6.1.3 TIME does not warrant (other than as set out in Paragraph 4 of this Service Schedule) that the MSE's performance will be uninterrupted, error-free and that there will be no malfunctions, failures or other disruptions. Any losses arising from, related to or as a consequence of such interruption, error, malfunction, failure or disruption is absolutely excluded.

6.2 Managed WIFI Service type. If the Managed Service type subscribed is Managed WIFI Service, the following conditions shall apply:

6.2.1 Should Customer require TIME to carry out any additional work beyond the Standard Service Scope, TIME may do so and charge the Customer a fee for such additional work. Prior to executing the additional work requested, TIME will provide a quotation and if the Customer agrees such quotation will vary this Agreement.

6.2.2 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that the Managed Service will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality.

6.2.3 TIME does not warrant (other than as set out in Paragraph 4 of this Service Schedule) that the MSE's performance will be uninterrupted, error-free and that there will be no malfunctions, failures or other disruptions. Any losses arising from, related to or as a consequence of such interruption, error, malfunction, failure or disruption is absolutely excluded.

6.3 Wireless IPVPN Service type. If the Managed Service type subscribed is Wireless IPVPN Service, the following conditions shall apply:

6.3.1 **Duration:** Notwithstanding anything to the contrary herein, the Initial Service Term for this Managed Service type is thirty six (36) months from the SCD.

6.3.2 **Acknowledgement:** Customer acknowledges that this Managed Service relies on third party mobile operators, and that any early cessation or termination (whether for cause or otherwise) requires the Customer to pay the third-party mobile operator's charges.

6.3.3 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that the Managed Service will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality.

6.3.4 TIME does not warrant (other than as set out in Paragraph 4 of this Service Schedule) that the MSE's performance will be uninterrupted, error-free and that there will be no malfunctions, failures or other disruptions. Any losses arising from, related to or as a consequence of such interruption, error, malfunction, failure or disruption is absolutely excluded.

6.3.5 Should Customer require TIME to carry out any additional work beyond the Standard Service Scope, TIME may do so and charge the Customer a fee for such additional work. Prior to executing the additional work requested, TIME will provide a quotation and if the Customer agrees such quotation will vary this Agreement.

6.4 Managed Router Service type. If the Managed Service type subscribed is Managed Router, the following conditions shall apply:

6.4.1 Should Customer require TIME to carry out any additional work beyond the Standard Service Scope, TIME may do so and charge the Customer a fee for such additional work. Prior to executing the additional work requested, TIME will provide a quotation and if the Customer agrees such quotation will vary this Agreement.

6.4.2 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that the Managed Service will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality.

6.4.3 TIME does not warrant (other than as set out in Paragraph 4 of this Service Schedule) that the MSE's performance will be uninterrupted, error-free and that there will be no malfunctions, failures or other disruptions. Any losses arising from, related to or as a consequence of such interruption, error, malfunction, failure or disruption is absolutely excluded.

6.4.4 Different Standard Service Scope applies if the Customer subscribes for either physical router or virtual router of Managed Service type.

6.4.5 If virtual router is the type of Managed Service type subscribed:

(a) there is no MSE to be ordered and delivered to the Service Location and the virtual router is within the TIME Network.
(b) restoration of virtual router in the event of malfunctioning will be done as soon as reasonably practicable.
(c) TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that this Managed Service type (i.e. virtual router) will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality; and
(d) TIME does not provide on-site support and/or on-site vendor support.

6.5 DDoS Protection Service type. If the Managed Service type subscribed is DDoS Shield/Advanced DDoS Shield, then the following conditions apply:

6.5.1 TIME does not provide on-site support and/or on-site vendor support;
6.5.2 The legal and beneficial title to all equipment required by TIME to carry out and provide this Managed Service type shall at all TIMEs remain with TIME;
6.5.3 TIME does not guarantee that this Managed Service type will absolutely protect the Customer from a distributed denial of service attack and any losses that Customer experiences as a result of, arising out of, related to or as a consequence of a DDoS attack is absolutely excluded;
6.5.4 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that this Managed Service type will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality;
6.5.5 TIME will continue to mitigate on a best effort basis any DDoS attack that exceeds the allocated mitigation threshold; and
6.5.5 When DDoS attack exceeds the allocated mitigation threshold, TIME will perform a black-hole if the DDoS attack affects the TIME Network or TIME's other customers in order to protect TIME's Network or TIME's other customers, which may impact the provision of this Managed Service type.

6.6 Managed Virtual Firewall. If the Managed Service type to be subscribed is Managed Virtual Firewall, then the following conditions apply:

6.6.1 The Customer must subscribe for the Managed Service Type identified as Managed Router – virtual in this Service Schedule in order for the Managed Virtual Firewall to be activated and delivered to Customer;
6.6.2 TIME may suspend the provision of the Managed Virtual Firewall if the charges for Qualifying Service and/or the Managed Router (virtual) are either outstanding beyond the due date or a ground to suspend the Qualifying Service has arisen;
6.6.3 TIME does not provide on-site support and/or on-site vendor support;
6.6.4 The legal and beneficial title to all equipment required by TIME to carry out and provide this Managed Service type shall at all times remain with TIME;
6.6.5 TIME does not guarantee that this Managed Service type will absolutely protect the Customer from any attack or malicious traffic and any losses that Customer experiences as a result of, arising out of, related to or as a consequence of an attack or malicious traffic is absolutely excluded; and
6.6.7 TIME does not make any representations or warranty, whether express or implied, and excludes any implied warranties (whether arising by operation of Applicable Law, equity or common law) that this Managed Service type will achieve the expected functionality, will enable the operating environment to be error-free or uninterrupted, and/or is of a specified quality or of any quality.

6.7 TIME Security Advanced Monitoring. If the Managed Service type to be subscribed is TIME Security Advanced Monitoring, then the following conditions apply:

6.7.1 **Duration:** Notwithstanding anything to the contrary herein, the Initial Service Term for this Managed Service type is twenty four (24) months from the SCD.
6.7.2 TIME does not guarantee that the TSAM will correctly detect and identify all:
(a) security events and incidents;
(b) unauthorised access to customer networks;
(c) viruses;
(d) spam; and
(e) other types of attacks or issues.
6.7.3 The Customer must promptly inform the TSAM security analyst, as assigned by TIME to the Customer, if there are any issues found after subscribing to TSAM for immediate remediation.

6.7.4 The Customer shall provide TIME with a written notice, fourteen (14) business days in advance of any network security testing and investigation to be conducted within the Customer's network.

6.7.5 Upon the expiry of the Term in accordance with sub-clause 7.3 below:

(a) TIME will store system logs up to thirty (30) days from the date of expiry of the Term unless the Customer informs TIME in writing of their objection to the same prior to the SCD;

(b) The Customer may request an extraction of the system logs for the aforementioned thirty (30) day period;

(c) The Customer must pay a fee for this extraction, which shall be determined by TIME, upon request for the extraction of the system logs; and

(d) The Customer will not be able to request an extraction of the system logs upon the expiry of forty five (45) days after the expiry of the Term.

6.7.6 If this Managed Service type is eligible for a service level agreement ("**SLA")**, SLA shall be provided to the Customer separately.

6.7.7 To receive this Managed Service type, the Customer must at its own cost:

(a) obtain an appropriate connectivity service;

(b) ensure the service term of the connectivity service does not expire prior to the service term of the Customer's TSAM services; and

(c) complete changes to the Customer's network and resources as TIME may reasonably require, from TIME to TIME, to enable log and event data to be passed to TIME from the Customer infrastructure to TIME infrastructure using a method stipulated by TIME.

6.7.8 Paragraph 10 of this Service Schedule G: Enterprise Managed Services shall not be applicable to the TSAM service type.

6.8 AVM Enforce Cloud Managed Services. If the Managed Service type subscribed is AVM Enforce Cloud Managed Services, then the following conditions apply:

6.8.1 In this Paragraph 6.8:

(a) "**Business Day**" means Monday to Friday excluding Saturday, Sunday or any public holidays in the state of Selangor Darul Ehsan in Malaysia;

(b) "**Business Hours**" means the hours between 9.00am and 5.30pm on a Business Day;

(c) "**Incident Report**" or "**IR**" means the report which describes the Qualifying Incident and includes information such as the date and TIME that the Qualifying Incident was detected, Customer details, location of the Qualifying Incident, problem description, Trouble Tickets escalated to the Principal (if applicable) and the severity level of the Qualifying Incident as determined by TIME;

(d) "**Interruption**" means circumstance(s) where the Customer's operations/virtual resource interrupts, affects or causes issues to TIME's servers, or to TIME's other virtualised cloud tenant within the Qualifying Service on the same server or to TIME's infrastructure in general;

(e) "**Modified Code**" is defined as the programming or instruction code which has been altered or customised for a particular software application;

(f) "**MTTr**" is defined as mean time to respond. The "**MTTr for on-site**" set out in AVM Enforce Cloud Managed Services Support Structure is only applicable to the equipment stored at Customer's site specifically provisioned for the Qualifying Service subscribed by the Customer;

(g) "**MTTR**" is defined as mean time to repair;

(h) "**Principal**" means the manufacturer, developer, proprietor and/or appointed distributors of a third-party hardware, software, solution or service used for the purpose of provisioning of AVM Enforce Cloud Managed Services and/or its Qualifying Service;

(i) "**Qualifying Incident**" means any unplanned interruption to the subscribed AVM Enforce Cloud Managed Services or reduction in the quality arising during typical usage of the subscribed AVM Enforce Cloud Managed Services. It is defined according to the different levels of severity according to the level of impact the incident has over the subscribed AVM Enforce Cloud Managed Services as set out in the AVM Enforce Cloud Managed Services Support Structure of this Service Schedule; and

(j) "**Trouble Ticket**" means the ticket raised by the Customer in accordance to any service interruption or unavailability of the subscribed services.

6.8.2 The Customer must subscribe for the specific AVM Enforce Cloud Managed Services option in order for that specific AVM Enforce Cloud Managed Services to be activated and delivered to Customer.

6.8.3 The specific AVM Enforce Cloud Managed Services option subscribed by the Customer cannot be exchanged by the Customer with another AVM Enforce Cloud Managed Services option.

6.8.4 In relation to Managed Backup and DR Only service and Managed OS, Patching, Backup and DR service, if a reported problem is suspected to be related to Modified Code, TIME may, in its sole and absolute discretion, request that the Modified Code be removed, and restore Customer's data from the centralised backup system of the Qualifying Service.

6.8.5 The Customer acknowledges and agrees that where the provision of AVM Enforce Cloud Managed Services and/or its Qualifying Service involves the use of or is provided through the hardware, software, solution and/or service from a Principal, AVM Enforce Cloud Managed Services is also subject to the Principal's terms and conditions and the limitations of or associated with such hardware, software, solution and/or service from the Principal.

6.8.6 Where TIME in its absolute discretion, deems necessary to escalate a Qualifying Incident to the Principal for assistance, TIME's obligations under the AVM Enforce Cloud Managed Services Support Structure and the MTTR of TIME set out in this Service Schedule, shall not apply and workaround time will be determined by Principal.

6.8.7 **Incident Reporting, Measurement and Closure**

(a) **Incident Opening**: Customer must report all Qualifying Incidents to the Service Desk, where a Trouble Ticket with a reference number or identifier will be registered and opened, and TIME will advise such information to Customer.

(b) **Incident Closure**: TIME will inform Customer when it believes the Qualifying Incident is cleared, and subject to sub-paragraph (iii) below, will close the Trouble Ticket when either Customer confirms that the Qualifying Incident is cleared within twenty four (24) hours after being informed by TIME or TIME has closed the trouble ticket after unsuccessful attempts to contact Customer, by reasonable means, in relation to the Qualifying Incident and Customer has not responded within twenty four (24) hours following TIME's attempt.

(c) If Customer however, confirms that the Qualifying Incident is not cleared within twenty four (24) hours following being informed that the Qualifying Incident is cleared, the Trouble Ticket will remain open, and TIME will continue to work to resolve the Qualifying Incident.

(d) If TIME detects an issue with the AVM Enforce Cloud Managed Services, TIME will log a case and inform to the Customer accordingly.

6.8.8 **Fault Rectification.** As soon as the Customer becomes aware of any Qualifying Incident relating to the AVM Enforce Cloud Managed Services, the Customer must immediately report that fault to TIME.

(a) Where TIME is aware of an Interruption, TIME reserves the right to rectify such Interruption by re-provisioning the Customer's virtual resource or suspending such operations of the Customer.

(b) Where the Customer reports to TIME of an Interruption, and TIME upon investigation, finds out that the Interruption is caused by third-party solution or services that are not supplied by TIME, TIME will notify the Customer that the Interruption is outside the scope of the Manages Service and the Qualifying Service. Where this occurs TIME shall not be responsible for resolution of the Interruption.

6.8.9 The table below addresses the severity levels support structure ("**AVM Enforce Cloud Managed Services Support Structure**") for the AVM Enforce Cloud Managed Services and escalation matrix. TIME shall, from time to time, notify the Customer of any updates to TIME's fault reporting procedures and escalation matrix:

Severity Level	**Severity Description**	**MTTr / MTTR for off-site**	**MTTr for on-site**	**L1-to-L2 Escalation**	**L2-to-Principal Escalation**	**Report**
1	An incident with critical business impact on the Customer's primary business operation, where there is: (i) a critical functionality loss in the system (system/storage/network/infra down) rendering the system unusable; (ii) a substantial loss of Service resulting in the Customer's business operations being severely disrupted; and/or (iii) all or a substantial portion of the Customer's mission critical data is at a significant risk of loss or corruption, with no alternative or workaround immediately available.	15 min/4 hours	4 hours	30 min	Note: When the Qualifying Incident is escalated to the Principal, the MTTR is determined by the Principal.	IR (3 days from the date of the Trouble Ticket)
2	An incident with major business impact on the Customer's business	15 min/8 hours	4 hours	2 hours		IR (3 days from Customer's

Severity Level	Severity Description	MTTr / MTTR for off-site	MTTr for on-site	L1-to-L2 Escalation	L2-to-Principal Escalation	Report
	operation, where there is a partial loss of critical/urgent business function due to hardware problems or malfunction, resulting in a degradation of such business function.					request for the IR)
3	An incident with low impact on the Customer's business operation, where there is a loss of non-critical business function.	15 min/24 Business Hours	Next Business Day	3 hours		N/A
4	Service requests fulfilment for small changes or additions which have low risk, low cost and occur quite frequently (requests to add/increase/decrease/remove/change).	15 min/48 Business Hours	Next Business Day	1 Business Day		N/A
5	An enquiry for troubleshooting and guidelines causing little or no impact to customers business with no binding SLAs (customer enquiries).	15 min/7 Business Days	Not Applicable	2 Business Days		N/A

6.8.10 **Special Condition for DR Recovery Shared Office Space @ Cyberjaya service**
The space and/or seats for the DR Recovery Shared Office Space @ Cyberjaya service are available on a "first come, first served" basis, subject to TIME's absolute discretion in reassigning the space and/or seats and the availability of the space and/or seats at the time.

6.9 IGS Enforce Managed Services 24 x 7 x 365. If the Managed Service type subscribed is IGS Enforce Managed Services 24 x 7 x 365, then the following conditions apply:

6.9.1 In this Paragraph 6.9:

(a) "**Business Day**" means Monday to Friday excluding Saturday, Sunday or any public holidays in the state of Selangor Darul Ehsan in Malaysia;
(b) "**Business Hours**" means the hours between 9.00am and 5.30pm on a Business Day;

(c) "**Incident Report**" or "**IR**" means the report which describes the Qualifying Incident and includes information such as the date and time that the Qualifying Incident was detected, Customer details, location of the Qualifying Incident, problem description, Trouble Tickets escalated to the Principal (if applicable) and the severity level of the Qualifying Incident as determined by TIME;

(d) "**Interruption**" means circumstance(s) where the Customer's operations/virtual resource interrupts, affects or causes issues to TIME's servers, or to TIME's other virtualised cloud tenant within the Qualifying Service on the same server or to TIME's infrastructure in general;

(e) "**Modified Code**" is defined as the programming or instruction code which has been altered or customised for a particular software application;

(f) "**MTTr**" is defined as mean time to respond. The "MTTr for on-site" set out in IGS Enforce Managed Services 24 x 7 x 365 Support Structure is only applicable to the equipment stored at Customer's site specifically provisioned for the Qualifying Service subscribed by the Customer;

(g) "**MTTR**" is defined as mean time to repair;

(h) "**Principal**" means the manufacturer, developer, proprietor and/or appointed distributors of a third-party hardware, software, solution or service used for the purpose of provisioning of IGS Enforce Managed Services 24 x 7 x 365 and/or its Qualifying Service;

(i) "**Qualifying Incident**" means any unplanned interruption to the subscribed IGS Enforce Managed Services 24 x 7 x 365 or reduction in the quality arising during typical usage of the subscribed IGS Enforce Managed Services 24 x 7 x 365. It is defined according to the different levels of severity according to the level of impact the incident has over the subscribed IGS Enforce Managed Services 24 x 7 x 365 as set out in the IGS Enforce Managed Services 24 x 7 x 365 Support Structure of this Service Schedule; and

(j) "**Trouble Ticket**" means the ticket raised by the Customer in accordance to any service interruption or unavailability of the subscribed services.

6.9.2 The Customer must subscribe for the specific IGS Enforce Managed Services 24 x 7 x 365 option in order for that specific IGS Enforce Managed Services 24 x 7 x 365 to be activated and delivered to Customer.

6.9.3 The specific IGS Enforce Managed Services 24 x 7 x 365 option subscribed by the Customer cannot be exchanged by the Customer with another IGS Enforce Managed Services 24 x 7 x 365 option.

6.9.4 The Customer acknowledges and agrees that where the provision of AVM Enforce Cloud Managed Services and/or its Qualifying Service involves the use of or is provided through the hardware, software, solution and/or service from a Principal, AVM Enforce Cloud Managed Services is also subject to the Principal's terms and conditions and the limitations of or associated with such hardware, software, solution and/or service from the Principal.

6.9.5 Where TIME in its absolute discretion, deems necessary to escalate a Qualifying Incident to the Principal for assistance, TIME's obligations under the IGS Enforce Managed Services 24 x 7 x 365 Support Structure and the MTTR of TIME set out in this Service Schedule, shall not apply and workaround time will be determined by Principal.

6.9.6 **Incident Reporting, Measurement and Closure**

(a) **Incident Opening**: Customer must report all Qualifying Incidents to the Service Desk, where a Trouble Ticket with a reference number or identifier will be registered and opened, and TIME will advise such information to Customer.

(b) **Incident Closure**: TIME will inform Customer when it believes the Qualifying Incident is cleared, and subject to sub-paragraph (iii) below, will close the Trouble

Ticket when either Customer confirms that the Qualifying Incident is cleared within twenty four (24) hours after being informed by TIME or TIME has closed the trouble ticket after unsuccessful attempts to contact Customer, by reasonable means, in relation to the Qualifying Incident and Customer has not responded within twenty four (24) hours following TIME's attempt.

(c) If Customer however, confirms that the Qualifying Incident is not cleared within twenty four (24) hours following being informed that the Qualifying Incident is cleared, the Trouble Ticket will remain open, and TIME will continue to work to resolve the Qualifying Incident.

(d) If TIME detects an issue with the IGS Enforce Managed Services 24 x 7 x 365, TIME will log a case and inform to the Customer accordingly.

6.9.7 **Fault Rectification.** As soon as the Customer becomes aware of any Qualifying Incident relating to the IGS Enforce Managed Services 24 x 7 x 365, the Customer must immediately report that fault to TIME.

(a) Where TIME is aware of an Interruption, TIME reserves the right to rectify such Interruption by re-provisioning the Customer's virtual resource or suspending such operations of the Customer.

(b) Where the Customer reports to TIME of an Interruption, and TIME upon investigation, finds out that the Interruption is caused by third-party solution or services that are not supplied by TIME, TIME will notify the Customer that the Interruption is outside the scope of the Manages Service and the Qualifying Service. Where this occurs TIME shall not be responsible for resolution of the Interruption.

6.9.8 The table below addresses the severity levels support structure ("IGS Enforce Managed Services 24 x 7 x 365 Support Structure") for the IGS Enforce Managed Services 24 x 7 x 365 and escalation matrix. TIME shall, from time to time, notify the Customer of any updates to TIME's fault reporting procedures and escalation matrix:

Severity Level	Severity Description	MTTr / MTTR for off-site	MTTr for on-site	L1-to-L2 Escalation	L2-to-Principal Escalation	Report
1	An incident with critical business impact on the Customer's primary business operation, where there is: (i) a critical functionality loss in the system (system/storage/network/infra down) rendering the system unusable; (ii) a substantial loss of Service resulting in the Customer's business operations being severely disrupted; and/or (iii) all or a substantial portion of the Customer's mission critical data is at a	15 min/4 hours	4 hours	30 min	Note: When the Qualifying Incident is escalated to the Principal, the MTTR is determined by the Principal.	IR (3 days from the date of the Trouble Ticket)

Severity Level	Severity Description	MTTr / MTTR for off-site	MTTr for on-site	L1-to-L2 Escalation	L2-to-Principal Escalation	Report
	significant risk of loss or corruption, with no alternative or workaround immediately available.					
2	An incident with major business impact on the Customer's business operation, where there is a partial loss of critical/urgent business function due to hardware problems or malfunction, resulting in a degradation of such business function.	15 min/8 hours	4 hours	2 hours		IR (3 days from Customer's request for the IR)
3	An incident with low impact on the Customer's business operation, where there is a loss of non-critical business function.	15 min/24 Business Hours	Next Business Day	3 Business Hours		N/A
4	Service requests fulfilment for small changes or additions which have low risk, low cost and occur quite frequently (requests to add/increase/decrease/remove/change).	15 min/48 Business Hours	Next Business Day	1 Business Day		N/A
5	An enquiry for troubleshooting and guidelines causing little or no impact to customers business with no binding SLAs (customer enquiries).	15 min/7 Business Days	Not Applicable	2 Business Days		N/A

6.10 **AVM Fusion Cloud Managed Service**. If the Managed Service type subscribed is AVM Fusion Cloud Managed Service, then the following conditions apply:

6.10.1 In this Paragraph 6.10:

(a) "**Business Day**" means Monday to Friday excluding Saturday, Sunday or any public holidays in the state of Selangor Darul Ehsan in Malaysia;
(b) "**Business Hours**" means the hours between 9.00am and 5.30pm on a Business Day;
(c) "**Incident Report**" or "**IR**" means the report which describes the Qualifying Incident and includes information such as the date and time that the Qualifying Incident was detected, Customer details, location of the Qualifying Incident, problem description, Trouble Tickets escalated to the Principal (if applicable) and the severity level of the Qualifying Incident as determined by TIME;
(d) "**Interruption**" means circumstance(s) where the Customer's operations/virtual resource interrupts, affects or causes issues to TIME's servers, or to TIME's other virtualised cloud tenant within the Qualifying Service on the same server or to TIME's infrastructure in general;
(e) "**Modified Code**" is defined as the programming or instruction code which has been altered or customised for a particular software application;
(f) "**MTTr**" is defined as mean time to respond. The "**MTTr for on-site**" set out in AVM Fusion Cloud Managed Service Support Structure is only applicable to the equipment stored at Customer's site specifically provisioned for the Qualifying Service subscribed by the Customer;
(g) "**MTTR**" is defined as mean time to repair;
(h) "**Principal**" means the manufacturer, developer, proprietor and/or appointed distributors of a third-party hardware, software, solution or service used for the purpose of provisioning of AVM Fusion Cloud Managed Service and/or its Qualifying Service;
(i) "**Qualifying Incident**" means any unplanned interruption to the subscribed AVM Fusion Cloud Managed Service or reduction in the quality arising during typical usage of the subscribed AVM Fusion Cloud Managed Service. It is defined according to the different levels of severity according to the level of impact the incident has over the subscribed AVM Fusion Cloud Managed Service as set out in the AVM Fusion Cloud Managed Service Support Structure of this Service Schedule; and
(j) "**Trouble Ticket**" means the ticket raised by the Customer in accordance to any service interruption or unavailability of the subscribed services.

6.10.2 The Customer acknowledges and agrees that where the provision of AVM Fusion Cloud Managed Service and/or its Qualifying Service involves the use of or is provided through the hardware, software, solution and/or service from a Principal, AVM Fusion Cloud Managed Service is also subject to the Principal's terms and conditions and the limitations of or associated with such hardware, software, solution and/or service from the Principal.

6.10.3 Where TIME in its absolute discretion, deems necessary to escalate a Qualifying Incident to the Principal for assistance, TIME's obligations under the AVM Fusion Cloud Managed Service Support Structure and the MTTR of TIME set out in this Service Schedule, shall not apply and workaround TIME will be determined by Principal.

6.10.4 **Incident Reporting, Measurement and Closure**

(a) **Incident Opening**: Customer must report all Qualifying Incidents to the Service Desk, where a Trouble Ticket with a reference number or identifier will be registered and opened, and TIME will advise such information to Customer.
(b) **Incident Closure**: TIME will inform Customer when it believes the Qualifying Incident is cleared, and subject to sub-paragraph (iii) below, will close the Trouble Ticket when either Customer confirms that the Qualifying Incident is cleared within twenty four (24) hours after being informed by TIME or TIME has closed the trouble ticket after unsuccessful attempts to contact Customer, by reasonable means, in

relation to the Qualifying Incident and Customer has not responded within twenty four (24) hours following TIME's attempt.

(c) If Customer however, confirms that the Qualifying Incident is not cleared within twenty four (24) hours following being informed that the Qualifying Incident is cleared, the Trouble Ticket will remain open, and TIME will continue to work to resolve the Qualifying Incident.

(d) If TIME detects an issue with the AVM Fusion Cloud Managed Service, TIME will log a case and inform to the Customer accordingly.

6.10.5 **Fault Rectification.** As soon as the Customer becomes aware of any Qualifying Incident relating to the AVM Fusion Cloud Managed Service, the Customer must immediately report that fault to TIME.

(a) Where TIME is aware of an Interruption, TIME reserves the right to rectify such Interruption by re-provisioning the Customer's virtual resource or suspending such operations of the Customer.

(b) Where the Customer reports to TIME of an Interruption, and TIME upon investigation, finds out that the Interruption is caused by third-party solution or services that are not supplied by TIME, TIME will notify the Customer that the Interruption is outside the scope of the Manages Service and the Qualifying Service. Where this occurs TIME shall not be responsible for resolution of the Interruption.

6.10.6 The table below addresses the severity levels support structure ("**AVM Fusion Cloud Managed Service Support Structure**") for the AVM Fusion Cloud Managed Service and escalation matrix. TIME shall, from time to time, notify the Customer of any updates to TIME's fault reporting procedures and escalation matrix:

Severity Level	**Severity Description**	**MTTr / MTTR for off-site**	**MTTr for on-site**	**L1-to-L2 Escalation**	**L2-to-Principal Escalation**	**Report**
1	An incident with critical business impact on the Customer's primary business operation, where there is: (i) a critical functionality loss in the system (system/storage/network/infra down) rendering the system unusable; (ii) a substantial loss of Service resulting in the Customer's business operations being severely disrupted; and/or (iii) all or a substantial portion of the Customer's mission critical data is at a significant risk of loss or corruption, with no	15 min/4 hours	4 hours	30 min	Note: When the Qualifying Incident is escalated to the Principal, the MTTR is determined by the Principal.	IR (3 days from the date of the Trouble Ticket)

Severity Level	Severity Description	MTTr / MTTR for off-site	MTTr for on-site	L1-to-L2 Escalation	L2-to-Principal Escalation	Report
	alternative or workaround immediately available.					
2	An incident with major business impact on the Customer's business operation, where there is a partial loss of critical/urgent business function due to hardware problems or malfunction, resulting in a degradation of such business function.	15 min/8 hours	4 hours	2 hours		IR (3 days from Customer's request for the IR)
3	An incident with low impact on the Customer's business operation, where there is a loss of non-critical business function.	15 min/24 Business Hours	Next Business Day	3 hours		N/A
4	Service requests fulfilment for small changes or additions which have low risk, low cost and occur quite frequently (requests to add/increase/decrease/remove/change).	15 min/48 Business Hours	Next Business Day	1 Business Day		N/A
5	An enquiry for troubleshooting and guidelines causing little or no impact to customers business with no binding SLAs (customer enquiries).	15 min/7 Business Days	Not Applicable	2 Business Days		N/A

6.10.7 **Customer's Responsibilities**. Where the provisioning of the Qualifying Service is on the Customer's own virtual machine (being used as the backup server), the Customer acknowledges and agrees that the Customer will be responsible for the following at all times and at its own expense:

(a) ensure that its own server, network, operating system, storage, firewall and applications, and all support services thereto are available for the purposes of the provisioning of the Qualifying Service;
(b) ensure the hardware, storage and backup infrastructure used by the Customer are configured for purposes of and compatible with the provisioning of the Qualifying Service; and
(c) ensure that TIME is provided with access to and use of the Customer's virtual machine for purposes of the provisioning of the AVM Fusion Cloud Managed Service.

6.11 TIME WAF. If the Managed Service type to be subscribed is TIME WAF, then the following conditions apply:

6.11.1 TIME may suspend the provision of the TIME WAF service if the charges for Qualifying Service are either outstanding beyond the due date or a ground to suspend the Qualifying Service has arisen;

6.11.2 The legal and beneficial title to all equipment required by TIME to carry out and provide this Managed Service type shall at all times remain with TIME; and

6.11.3 TIME does not guarantee that this Managed Service type will absolutely protect the Customer from any attack or malicious traffic and any losses that Customer experiences as a result of, arising out of, related to or as a consequence of an attack or malicious traffic is absolutely excluded.

6.12 Network Insight Service. If the Managed Service type to be subscribed is Network Insight Service, then the following conditions shall apply:

6.12.1 Minimum contract period is 12 months;

6.12.2 For early termination/cancellation of the Service, the Customer shall give TIME 30 days prior written notice;

6.12.3 Cancellation charges of remaining contract shall apply if the Service is cancelled/terminated before the expiration of the contract;

6.12.4 Upon early termination/cancellation of the Service for whatever reason, the Customer shall forthwith pay TIME the Penalty Charges and all Balance Charges for the remainder of the contract period; and

6.12.5 Upgrade of bandwidth is permitted anyTIME during the Service period.

6.13 Managed SD-WAN Service. If the Managed Service type to be subscribed is TIME Managed SD-WAN packages, then the following conditions shall apply:

6.13.1 Minimum contract period is 24 months;

6.13.2 For early termination/cancellation of the Service, the Customer shall give TIME 30 days prior written notice;

6.13.3 Upon early termination/cancellation of the Service for whatever reason, the Customer shall forthwith pay TIME the Penalty Charges and all Balance Charges for the remainder of the contract period;

6.13.4 SD-WAN Premier package and SD-WAN Basic package are mandatory to be subscribed together;

6.13.5 For SD-WAN Lite package, Customer is required to subscribe it with either SD-WAN Premier or SD-WAN Basic package. In addition, it is mandatory to have at least two (2) office lines/sites subscribed to SD-WAN Premier or Basic package; and

6.13.6 All lines/sites are required to use the same router brand.

6.14 TIME Secure DNS. If the Managed Service type to be subscribed is TIME Secure DNS, then the following conditions apply:

6.14.1 TIME may suspend the provision of the TIME Secure DNS service if the charges for Qualifying Service are either outstanding beyond the due date or a ground to suspend the Qualifying Service has arisen;

6.14.2 The legal and beneficial title to all equipment required by TIME to carry out and provide this Managed Service type shall at all times remain with TIME; and

6.14.3 TIME does not guarantee that this Managed Service type will absolutely protect the Customer fom any attack or malicious traffic and any losses that Customer experiences as a result of, arising out of, related to or as a consequence of an attack or malicious traffic is absolutely excluded.

6.15 **TIME Cloud Managed Service** If the Managed Service type subscribed is Cloud Managed Service, then the following conditions apply:

6.15.1 In this Paragraph 6.15:

(a) "**Business Day**" means Monday to Friday excluding Saturday, Sunday or any public holidays in the state of Selangor Darul Ehsan in Malaysia;

(b) "**Business Hours**" means the hours between 9.00am and 5.30pm on a Business Day;

(c) "**Incident Report**" or "**IR**" means the report which describes the Qualifying Incident and includes information such as the date and time that the Qualifying Incident was detected, Customer details, location of the Qualifying Incident, problem description, Trouble Tickets escalated to the Principal (if applicable) and the severity level of the Qualifying Incident as determined by TIME;

(d) "**Interruption**" means circumstance(s) where the Customer's operations/virtual resource interrupts, affects or causes issues to TIME's servers, or to TIME's other virtualised cloud tenant within the Qualifying Service on the same server or to TIME's infrastructure in general;

(e) "**Modified Code**" is defined as the programming or instruction code which has been altered or customised for a particular software application;

(f) "**MTTr**" is defined as mean time to respond. The "MTTr for on-site" set out in Cloud Managed Services Support Structure is only applicable to the equipment stored at Customer's site specifically provisioned for the Qualifying Service subscribed by the Customer;

(g) "**MTTR**" is defined as mean time to repair;

(h) "**Principal**" means the manufacturer, developer, proprietor and/or appointed distributors of a third-party hardware, software, solution or service used for the purpose of provisioning of Cloud Managed Services and/or its Qualifying Service;

(i) "**Qualifying Incident**" means any unplanned interruption to the subscribed Cloud Managed Services or reduction in the quality arising during typical usage of the subscribed Cloud Managed Services. It is defined according to the different levels of severity according to the level of impact the incident has over the subscribed Cloud Managed Services as set out in the Cloud Managed Services Support Structure of this Service Schedule; and

(j) "**Trouble Ticket**" means the ticket raised by the Customer in accordance to any service interruption or unavailability of the subscribed services.

6.15.2 The Customer must subscribe for the specific Cloud Managed Services option in order for that specific Cloud Managed Services to be activated and delivered to Customer.

6.15.3 The specific Cloud Managed Services option subscribed by the Customer cannot be exchanged by the Customer with another Cloud Managed Services option.

6.15.4 In relation to Managed OS, Patching, Backup & Restore and DR service, if a reported problem is suspected to be related to Modified Code, TIME may, in its sole and absolute discretion, request that the Modified Code be removed, and restore Customer's data from the centralised backup system of the Qualifying Service.

6.15.5 The Customer acknowledges and agrees that where the provision of Cloud Managed Services and/or its Qualifying Service involves the use of or is provided through the hardware, software, solution and/or service from a Principal, Cloud Managed Services is also subject to the Principal's terms and conditions and the limitations of or associated with such hardware, software, solution and/or service from the Principal.

6.15.6 Where TIME in its absolute discretion, deems necessary to escalate a Qualifying Incident to the Principal for assistance, TIME's obligations under the Cloud Managed Services Support Structure and the MTTR of TIME set out in this Service Schedule, shall not apply and workaround time will be determined by Principal.

6.15.7 Incident Reporting, Measurement and Closure

(a) Incident Opening: Customer must report all Qualifying Incidents to the Service Desk, where a Trouble Ticket with a reference number or identifier will be registered and opened, and TIME will advise such information to Customer.
(b) Incident Closure: TIME will inform Customer when it believes the Qualifying Incident is cleared, and subject to sub-paragraph (iii) below, will close the Trouble Ticket when either Customer confirms that the Qualifying Incident is cleared within twenty four (24) hours after being informed by TIME or TIME has closed the trouble ticket after unsuccessful attempts to contact Customer, by reasonable means, in relation to the Qualifying Incident and Customer has not responded within twenty four (24) hours following TIME's attempt.
(c) If Customer however, confirms that the Qualifying Incident is not cleared within twenty four (24) hours following being informed that the Qualifying Incident is cleared, the Trouble Ticket will remain open, and TIME will continue to work to resolve the Qualifying Incident.
(d) If TIME detects an issue with the Cloud Managed Services, TIME will log a case and inform to the Customer accordingly.

6.15.8 Fault Rectification. As soon as the Customer becomes aware of any Qualifying Incident relating to the Cloud Managed Services, the Customer must immediately report that fault to TIME.

(a) Where TIME is aware of an Interruption, TIME reserves the right to rectify such Interruption by re-provisioning the Customer's virtual resource or suspending such operations of the Customer.

(b) Where the Customer reports to TIME of an Interruption, and TIME upon investigation, finds out that the Interruption is caused by third-party solution or services that are not supplied by TIME, TIME will notify the Customer that the Interruption is outside the scope of the Manages Service and the Qualifying Service. Where this occurs TIME shall not be responsible for resolution of the Interruption.

6.15.9 The table below addresses the severity levels support structure ("Cloud Managed Services Support Structure") for the Cloud Managed Services and escalation matrix. TIME shall, from time to time, notify the Customer of any updates to TIME's fault reporting procedures and escalation matrix:

Severity Level	**Severity Description**	**MTTr / MTTR for off-site**	**MTTr for on-site**	**L1-to-L2 Escalation**	**L2-to-Principal Escalation**	**Report**
1	An incident with critical business impact on the Customer's primary business operation, where there is: (i) a critical functionality loss in the system (system/storage/network/infra down) rendering the system unusable; (ii) a substantial loss of Service resulting in the Customer's business operations being severely disrupted; and/or (iii) all or a substantial portion of the Customer's mission critical data is at a significant risk of loss or corruption, with no alternative or workaround immediately available.	15 min/4 hours	4 hours	30 min	Note: When the Qualifying Incident is escalated to the Principal, the MTTR is determined by the Principal.	IR (3 days from the date of the Trouble Ticket)
2	An incident with major business impact on the Customer's business	15 min/8 hours	4 hours	2 hours		IR (3 days from Customer's

Severity Level	Severity Description	MTTr / MTTR for off-site	MTTr for on-site	L1-to-L2 Escalation	L2-to-Principal Escalation	Report
	operation, where there is a partial loss of critical/urgent business function due to hardware problems or malfunction, resulting in a degradation of such business function.					request for the IR)
3	An incident with low impact on the Customer's business operation, where there is a loss of non-critical business function.	15 min/24 Business Hours	Next Business Day	3 hours		N/A
4	Service requests fulfilment for small changes or additions which have low risk, low cost and occur quite frequently (requests to add/increase/decrease/remove/change).	15 min/48 Business Hours	Next Business Day	1 Business Day		N/A
5	An enquiry for troubleshooting and guidelines causing little or no impact to customers business with no binding SLAs (customer enquiries).	15 min/7 Business Days	Not Applicable	2 Business Days		N/A

6.16 **TIME PAM**. If the Managed Services type to be subscribed is TIME PAM, then the following conditions apply:

6.16.1 TIME may suspend the provision of the TIME PAM service if the charges for Qualifying Service are either outstanding beyond the due date or a ground to suspend the Qualifying Service has arisen;

6.16.2 The legal and beneficial title to all equipment / firmware required by TIME to carry out and provide this Managed Service type shall at all times remain with TIME; and

6.16.3 TIME does not guarantee that this Managed Service type will absolutely protect the Customer from any attack or malicious traffic and any losses that Customer experiences.

6.17 **TIME MEN**

6.17.1 TIME may suspend the provision of the TIME MEN service if the charges for Qualifying Service are either outstanding beyond the due date or a ground to suspend the Qualifying Service has arisen;

6.17.2 The legal and beneficial title to all equipment / firmware required by TIME to carry out and provide this Managed Service type shall at all times remain with TIME; and

6.17.3 TIME does not guarantee that this Managed Service type will absolutely protect the Customer from any attack or malicious traffic and any losses that Customer experiences for the subscription with network security whether as bundle or value-added services.

6.18 **TIME VA**

6.18.1 Minimum contract period is 12 months;

6.18.2 TIME will invoice the Customer quarterly upon the completion of the VA scan for each respective quarter;

6.18.3 For early termination/cancellation of the TIME VA Service during the Initial Service Term, the Customer shall give TIME 30 days prior written notice, and the Customer shall pay TIME the outstanding Charges, Balance Charges, and Cancellation Costs or Termination Charges (as the case may be);

6.18.4 During the Renewed Service Term, should the Customer wish to terminate the TIME VA Services from the next scheduled quarterly VA scan onward, the Customer shall give TIME at least 30 days written notice prior to the immediately preceding quarterly VA scan. If the notice is given less than 30 days before the preceding quarterly VA scan, TIME will still proceed with the next scheduled quarterly VA scan, and the termination will only take effect from the subsequent quarterly VA scanning cycle following the next scheduled quarterly VA scan;
For illustration purposes, if the Customer wishes to terminate the TIME VA Services for the next quarterly VA scan scheduled on 30 June 2024, the latest the Customer is required to give written notice to TIME is 30 days before the preceding quarterly VA scan conducted on 31 March 2024, which is 1 March 2024. If the Customer provides written notice later than 1 March 2024, TIME will still conduct the quarterly VA scan on 30 June 2024 and the termination will only take effect for the subsequent quarterly VA scan on 31 August 2024. For the avoidance of doubt, under all circumstances, the quarterly scan on 31 March 2024 will be conducted and invoiced to the Customer accordingly.

6.18.5 TIME may suspend the provision of the TIME VA service if the charges for Qualifying Service are either outstanding beyond the due date or a ground to suspend the Qualifying Service has arisen;

6.18.6 The legal and beneficial title to all equipment / firmware required by TIME to carry out and provide this Managed Service type shall at all times remain with TIME; and

6.18.7 TIME's responsibility is only to provide the vulnerability scanning result with advisory based on scanning result. The remediation action to solve the identified vulnerability is customer responsibility, unless the platform services is provided by TIME as managed services (limited to scope of work (SOW) of the managed services only).

6.18.8 TIME does not guarantee that this Managed Service type will absolutely protect the Customer from any attack or malicious traffic and any losses that Customer experiences.

6.19 TIME MDR

6.19.1 Minimum contract period is 12 months.

6.19.2 TIME does not guarantee that the TIME MDR will correctly detect and identify all:
(a) security events and incidents;
(b) unauthorised access to customer networks;
(c) viruses;
(d) spam; and
(e) other types of attacks or issues.

6.19.3 The Customer must promptly inform the TIME MDR security analyst, if there are any issues found after subscribing to TIME MDR for immediate remediation.

6.19.4 The Customer shall provide TIME with a written notice, fourteen (14) business days in advance of any network security testing and investigation to be conducted within the Customer's network.

6.19.5 Upon the expiry of the Term in accordance with sub-clause 7.3 below:
(a) TIME will store system logs up to thirty (30) days from the date of expiry of the Term unless the Customer informs TIME in writing of their objection to the same prior to the SCD;
(b) The Customer may request an extraction of the system logs for the aforementioned thirty (30) day period;
(c) The Customer must pay a fee for this extraction, which shall be determined by TIME, upon request for the extraction of the system logs; and
(d) The Customer will not be able to request an extraction of the system logs upon the expiry of forty five (45) days after the expiry of the Term.

6.19.6 If this Managed Service type is eligible for a service level agreement ("**SLA")**, SLA shall be provided to the Customer separately.

6.19.7 To receive this Managed Service type, the Customer must at its own cost:
(a) obtain an appropriate connectivity service;
(b) ensure the service term of the connectivity service does not expire prior to the service term of the Customer's MDR services; and
(c) complete changes to the Customer's network and resources as TIME may reasonably require, from TIME to TIME, to enable log and event data to be passed

to TIME from the Customer infrastructure to TIME infrastructure using a method stipulated by TIME.

6.19.8 Paragraph 10 of this Service Schedule G: Enterprise Managed Services shall not be applicable to the MDR service type.

6.19.9 It is Customer's responsibility to ensure that their contact information is correct and any changes to the escalation paths should be communicated to TIME with urgency.

6.19.10 To resolve escalated alerts, the Customer is responsible for responding to escalated alerts and comments promptly.

6.19.11 The Customer is responsible for escalating alerts back to TIME that require action or analysis by the SOC for alerts that are assigned to the client after analysis.

6.19.12 It is the sole responsibility of the Customer to communicate in advance on any changes to the service environment and/or devices during the engagement period that may impact the service of TIME.

6.19.13 TIME will determine if the alerts or security events warrant alert classification or escalation being responsible for alert analysis and investigation.

6.19.14 In accordance with the established SLAs, TIME will investigate all initial security alerts identified and escalate alerts as deemed appropriate.

6.19.15 TIME will escalate the alert to the Client for action, if one or more events require Client escalation.

6.19.16 TIME will perform alert triage to include determining categorization and prioritization of the alert.

6.19.17 It is TIME's responsibility to create and investigate alerts as events are pulled into the incident management workflow.

6.19.18 As TIME is responsible for alert escalation and response, only TIME has the authority to investigate events or alerts to ensure due diligence of event investigation and accountability in reporting.

6.19.19 Exclusions

(a) Events not forwarded/ received by TIME to:

(i) An error or delay from Client.
(ii) Failure to generate logged events due to system failure of the network environment, internet connectivity and related issues.
(iii) Inability to provide a suitable and secure environment for on-premises devices.

(b) Delays or interruptions to service, deficiencies, and degradations, due to:

(i) Internet or private access supplied by Client.
(ii) Any equipment, systems including power or services not covered in the service contract.

(iii) Any equipment, configuration, routing event, or technology within the management or in control of the Client related to the delivery of services offered by TIME.
(iv) Changes to the system specifications by Client.
(v) Adjustments or removal of a service component by Client without consent by mutual agreement.
(vi) Negligence, omissions or acts of third parties of Client that impact the services offered by TIME.
(vii) Undertaking of scheduled or emergency maintenance.
(viii) Changes or outages to network, software, or server to the managed services environment without reasonable prior notification that significantly impact event volumes. Applicable to any asset that may be affected with the generation and/ or transmission capability of logs, and events or other activity which is monitored by TIME for security alerts.

(c) Non-compliance by Client or related parties to the instructions provided by TIME, regarding:

(i) The deployment, adjustment, or maintenance of any software, policy, or license.
(ii) Recommended configurations on managed or unmanaged equipment that impacts the provision of MDR Services.

(d) Duplication of services that may impact efficiency, due to the presence of multiple software/ agents within a given environment or asset.

6.20 TIME Secure Network

If the Managed Service type subscribed is TIME Secure Network, the following conditions apply:

6.20.1 Dependency

(a) TIME Secure Network may only be subscribed to where the Customer maintains an active Internet Direct service with a fixed public IP address assigned by TIME.

(b) Suspension or termination of the Internet Direct service shall automatically result in suspension or termination of TIME Secure Network.

6.20.2 Nature of Service

TIME Secure Network is a network-based threat communication visibility service formed based on the fixed public IP address assigned by TIME under the subscribed Internet Direct service.

The service:

(a) Utilises NetFlow or equivalent network telemetry generated within TIME's network infrastructure;

(b) Correlates traffic associated with the assigned fixed public IP address against threat intelligence databases;

(c) Provides dashboard visibility of detected suspicious or malicious communications;

(d) Operates in a non-inline architecture and does not block, filter, drop, modify or otherwise interfere with Customer traffic.

6.20.3 Service Limitations

(a) Is limited to traffic observable within TIME's network and associated with the Customer's assigned fixed public IP address;

(b) Does not provide visibility of internal network traffic (east-west traffic);

(c) Does not inspect encrypted payload content; TIME processes network metadata only and does not inspect payload content unless otherwise expressly stated.

(d) Does not include traffic blocking, enforcement, incident response, forensic investigation, endpoint monitoring or remediation services.

(e) TIME Secure Network is dependent on availability and accuracy of network telemetry generated within TIME's infrastructure. Temporary interruption of telemetry collection, maintenance activities, or infrastructure upgrades may result in temporary unavailability of dashboard data without constituting a service failure.

6.20.4 Service Guarantees

(a) TIME does not guarantee detection of all malicious traffic, security incidents, unauthorized access, malware, botnet activity or data exfiltration attempts.

(b) The service operates on a best-effort basis and is dependent on available threat intelligence sources and observable network telemetry.

6.20.5 Maintenance Window

TIME may perform firmware updates, patching, or maintenance activities during scheduled maintenance windows. Planned maintenance shall not constitute service failure.

6.20.6 Data Retention

Threat event logs and dashboard historical data shall be retained for a period of 7 days unless otherwise specified in the Service Order.

TIME is not obligated to retain or provide historical logs beyond the defined retention period.

6.20.7 Customer Responsibility

(a) The Customer remains responsible for reviewing dashboard alerts and taking appropriate action within its internal environment.

(b) TIME shall not be liable for losses arising from threats not detected or from failure by the Customer to act upon detected events.

6.21 **TIME Secure Network+**

6.21.1 Dependency

TIME Secure Network+ may only be subscribed to where the Customer maintains:

(a) An active Internet Direct service with a fixed public IP address assigned by TIME; and

(b) An active TIME Secure Network service.

Suspension or termination of Internet Direct or TIME Secure Network shall automatically result in suspension or termination of TIME Secure Network+.

6.21.2 Environmental Dependency

(a) Customer shall provide adequate rack space, stable power supply, cooling, and physical security for the deployed appliance.

(b) TIME shall not be liable for failure arising from environmental or power-related issues at the Service Location.

6.21.3 Nature of Service

TIME Secure Network+ is an inline network threat enforcement service deployed within the Customer's network environment.

The service:

(a) Is provisioned using DarkShield security appliance(s) installed at the Service Location;

(b) Is positioned inline between the Internet Direct termination point and the Customer's firewall infrastructure;

(c) Performs real-time inspection and correlation of traffic associated with the assigned fixed public IP address against threat intelligence databases and configured enforcement policies;

(d) May block, drop or restrict malicious traffic in accordance with configured security policies

(e) The DarkShield appliance operates in fail-safe mode. In the event of appliance malfunction or system failure, traffic will bypass enforcement in order to maintain Internet connectivity.

(f) During fail-safe operation, enforcement protection will not be active until normal operation is restored.

6.21.4 Service Limitations

(a) Is limited to traffic that passes through the deployed appliance; TIME shall not be responsible for traffic that bypasses the appliance due to Customer network design, reconfiguration, routing changes, or misconfiguration.

(b) Enforcement capability is limited to the subscribed interface capacity (up to 1Gbps per instance). Where Customer Internet Direct bandwidth exceeds the enforcement capacity, Customer shall be responsible for subscribing to additional instances or upgraded capacity. TIME shall not be liable for performance degradation resulting from capacity exceedance.

(c) Enforcement actions are based on predefined threat intelligence feeds and configured security policies. TIME shall not be liable for any business interruption arising from false positives, policy-based blocking, or automated enforcement actions carried out in accordance with configured policies.

(d) Does not provide visibility or enforcement of internal network traffic (east-west traffic);

(e) Does not include endpoint protection, forensic investigation, vulnerability remediation or managed detection and response services;

(f) Does not guarantee prevention of all malicious traffic or security incidents.

The service operates on a best-effort basis within the technical constraints of the deployed DarkShield platform and Customer network configuration.

6.22 **TIME Network Analytics.**

If the Managed Service type to be subscribed is TIME Network Analytics, then the following conditions apply:

6.22.1 Dependency

(a) TIME Network Analytics may only be subscribed to where the Customer maintains an active Qualifying Service with TIME.

(b) Suspension or termination of the Qualifying Service shall automatically result in suspension or termination of TIME Network Analytics without any liability on the part of TIME

6.22.2 Nature of Service

(a) TIME Network Analytics is a PRTG-based network performance monitoring and analytics service that provides visibility of key performance metrics on subscribed TIME Managed CPE, delivered via a self-serve web-based dashboard hosted on TIME Cloud.

(b) The service provides monitoring and visibility only. It does not include traffic blocking, active remediation, endpoint protection, or incident response capabilities.

(c) The service is applicable only to TIME Managed CPE, including routers, firewalls, and SD-WAN devices. Customer-owned LAN network devices may be included as an optional add-on, subject to scope evaluation. Third party carrier and telco connectivity monitoring are expressly out of scope.

(c) TIME Network Analytics is dependent on the availability and accuracy of data collected from the Customer's device(s) via SNM , Netflow v9 or VPN access. Temporary interruption of data collection, maintenance activities, or infrastructure upgrades may result in temporary unavailability of dashboard data without constituting a service failure.

6.22.3 Contract

(a) Minimum contract period is twelve (12) months.
(b) For early termination/cancellation of the Service, the Customer shall give TIME 30 days prior written notice;
(c) Cancellation charges of remaining contract shall apply if the Service is cancelled/terminated before the expiration of the contract;
(d) Upon early termination/cancellation of the Service for whatever reason, the Customer shall forthwith pay TIME the Penalty Charges and all Balance Charges for the remainder of the contract period; and

6.22.4 Deployment Scope

(a) The Standard Package covers one (1) TIME Managed CPE device per subscription with five (5) sensors. Additional devices and add-on sensors may be provisioned at the applicable rates and are subject to scope evaluation by TIME, including assessment of complexity, device types, sites, and integrations.

(b) The service applies primarily only to TIME Managed CPE, including routers, firewalls, and SD-WAN devices. Customer-owned LAN network devices may be included as an optional add-on, subject to scope evaluation. Third party carrier and telco connectivity monitoring are expressly out of scope.

(c) TIME shall determine the suitability of any device for inclusion in the service scope and reserves the right to decline inclusion of any device that does not meet the technical pre-requisites or that TIME reasonably considers incompatible with the service platform.

6.22.5 Customer Responsibilities

The Customer acknowledges that the delivery of the Service is dependent on the Customer's network environment, devices, and configurations. The Customer shall remain responsible for the operation, configuration, and maintenance of its network and equipment at all times.

Without limiting the Customer's obligations under the Agreement, the Customer shall, at its own cost and throughout the Contract Term, including but not limited to, ensure the following:-

(a) ensure that all subscribed device(s) maintain a reachable public or private IP address, have SNMP enabled, and provide VPN access where required by TIME for sensor connectivity;

(b) notify TIME in writing at least fourteen (14) days in advance of any planned changes to the network environment, device configurations, or IP addressing that may affect the delivery of the service;

(c) review the self-serve dashboard and respond to alerts and notifications issued by TIME in a timely manner; and

(d) ensure that its contact information and escalation paths are kept current and any changes are communicated to TIME promptly.

6.22.6 Service Guarantees

(a) TIME does not guarantee detection of all network performance issues, faults, or degradation events.

(b) The service operates on a best-effort basis and is dependent on the accessibility, availability and accuracy of data collected from the Customer's subscribed device(s).

6.22.7 Platform and Data Retention

(a) The service is hosted on TIME Cloud. TIME may perform scheduled maintenance, patching, or upgrades to the platform. Planned maintenance shall not constitute a service failure.

(b) Historical data /records shall be retained for a period of thirty (30) days unless otherwise specified in the Service Order. TIME shall have no obligation to retain or provide data beyond the defined retention period.

6.22.8 Service Limitations and Exclusions

TIME shall not be liable for any failure to detect or notify the Customer of any event arising from or attributable to:

(a) the Customer's device(s) or VPN being unreachable or inaccessible;

(b) SNMP misconfiguration, incorrect configuration, or disabling of SNMP on the Customer's device(s);

(c) Netflow v9 misconfiguration, incorrect configuration, or disabling of Netflow v9 on the Customer's device(s);

(d) network or device configuration changes made by the Customer without prior notification to TIME; or

(e) any device or connectivity that is expressly outside of the defined service scope.

6.22.9 Alarm Monitoring and Escalation Structure

The table below sets out the alarm severity levels and TIME's monitoring and escalation obligations for TIME Network Analytics:

Severity Level	Service Layer	Severity Description	TIME Action	Customer Notification	Report
1	Platform / Sensor Layer	Platform unavailable or one or more sensors in Down state - sensor is no longer reachable, collecting, or reporting data and no statistics are being displayed on the Customer's dashboard. All sensor-related failures, regardless of which metric is affected, are classified as Severity 1. This does not reflect the performance state of the Customer's network or devices.	TIME will investigate and notify Customer via email upon detection.	Yes - email to Customer's nominated contact	Available on request
2	Platform / Sensor Layer	Sensor reachable but in Warning state - stale or incomplete data being returned. May indicate a connectivity issue between the sensor and the monitored device, or a device configuration change. Customer is advised to investigate	Customer to investigate via dashboard. TIME does not actively monitor or escalate.	No	Self-service

		device reachability and SNMP configuration.			
3	Metric / Performance Layer	Sensors operational and collecting data normally. One or more metrics showing warning-level readings. Customer to review dashboard and act accordingly.	Customer to review via dashboard. TIME does not actively monitor or escalate.	No	Self-service

PART B – SERVICE DELIVERY AND MANAGEMENT

7. OUR OBLIGATIONS

7.1 Service Delivery/Provisioning. Before and/or by the CRD or any revised CRD, TIME will:

7.1.1 comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at the Service Location(s) that are notified to TIME in writing, but TIME will not be liable if, as a result of any such compliance, TIME is in breach of any of its obligations under this Agreement;

7.1.2 provide you with contact details for the helpdesk that you will be able to contact to submit Service requests, report Incidents and ask questions about the Service (***"Service Desk"***);

7.1.3 **Supply of MSE.** In respect of Managed Service types that provides for MSE to be supplied to Customer by TIME, the following are our obligations:

(a) All MSE as specified in the Service Order or a quotation (for customised solution) of a type of Managed Service shall be procured, supplied and delivered to the Service Location as soon as reasonably practicable to meet the CRD;
(b) Quantity of MSE to be delivered by TIME is as specified in the quotation to Customer (whether it is Standard Service Scope or a customised scope);
(c) All MSE as specified in an accepted quotation will be ordered only after the Service Order has been accepted by TIME;
(d) If the type of MSE as specified by the Customer, requires TIME to place a special order with the third party vendor, the MSE will be delivered based on the delivery schedule specified by that third party vendor and the CRD will not be applicable; and
(e) If the quantity of MSE supplied is less than the agreed quantity in the quotation, TIME will make up the shortfall as quickly as possible.

7.1.4 **Installation and Configuration of the MSE**

(a) will use reasonable care and skill to install the MSE at the designated points or locations at the Service Location; and
(b) will use reasonable care and skill to configure the MSE to meet the requirements of the type of Managed Services.

7.1.5 Provision the TIME Network in order to provide the Managed Service;

7.1.6 Once provisioning of the Managed Service is completed, carry out the SAT that the Managed Service and/or the MSEs are operating within normal parameters;

7.1.7 Fine tuning the delivered services;

7.1.9 Provide a one-time hand-over training; and

7.1.10 Issue a notice to Customer specifying the SCD for the Managed Service if Paragraph 2.1.2 of this Service Schedule applies.

7.2 During Operation: On and from the SCD, TIME:

7.2.1 will perform and deliver the Managed Services to the best of its ability, professionally and with reasonable care and skill, and subject always to the terms in this Service Schedule;

7.2.2 will respond and use reasonable endeavours to remedy an Incident without undue delay if TIME detects or if you report an incident to the Service Desk;

7.2.3 may carry out any maintenance as may be specified in the Standard Service Scope (including to and/or upgrading of TIME's Network) from time to time and will endeavour to inform you at least five (5) days before any such maintenance work is to commence, however, TIME may inform you with less notice than normal where maintenance is required in an emergency;

7.2.4 update the firmware to the MSE and/or all necessary equipment in order to provide the Managed Service (as and when required and if technically appropriate); and

7.2.5 carry out the applicable Standard Service Scope.

7.3 The End of the Service: Upon expiry of the Term, TIME will:

7.3.1 cease providing the Managed Service;

7.3.2 provide to the Customer any documentation and manuals that are identified in the Standard Service Scope applicable to that Managed Service type; and

7.3.3 provide any MSE manuals that were provided by the vendors or manufacturers of the MSE to the Customer.

8 CUSTOMER'S OBLIGATIONS

8.1 Service Delivery: Before and/or by the CRD or any revised CRD, the Customer will:

8.1.1 provide all reasonable assistance to TIME in order that TIME may provision the Managed Service;

8.1.2 Do all things required and specified in Paragraph 3.1.1 above;

8.1.3 provide sufficient space at the Service Location to store, in a safe and secure manner, the MSE delivered by TIME;

8.1.4 provide TIME with the names and contact details of any individuals authorised to act on your behalf for Managed Service management matters ("Customer Contact"), but TIME may also accept instructions from a person who it reasonably believes is acting with your authority;

8.1.5 comply with the technical specifications in the use of the Managed Service as may be provided by TIME periodically; and

8.1.6 cooperate with TIME in order to achieve the CRD.

8.2 **During Operation:** On and from the SCD, you will:

8.2.1 Procure and maintain any licence, permit or authorisation (***"Permit"***) that you may require to use the Managed Service, but you agree to continue to pay the Charges even if you do not obtain such Permit;

8.2.2 Cooperate with TIME to enable TIME to carry out the Managed Service (where required);

8.2.3 comply with the incident reporting procedure that TIME provides you in respect of each type of Managed Service;

8.2.4 acknowledge that the MSE is under Customer's possession and/or control and undertake to take all reasonable care to ensure that the MSE is not damaged, destroyed, stolen and/or vandalised (fair wear and tear excepted);

8.2.5 control access to the MSE in order to minimise any unauthorised access thereto and take all reasonable steps to prevent unauthorised access to the MSE and/or the Managed Service;

8.2.6 not to do anything or not fail to do anything that may compromise the MSE by a third party (including causing any MSE to function as a bot); and

8.2.7 adhere to applicable requirements specified in Applicable Laws.

8.3 **The End of the Service:** On the expiry of the Term, you will:

8.3.1 if instructed by TIME in writing, disconnect any Customer Equipment from Service Equipment located at the Service Location.

9. USE AND REPLACEMENT OF PERSONNEL

9.1 Throughout the Term, TIME warrants that members of TIME Team assigned to perform the Managed Services are properly qualified.

9.2 In the event that Customer is dissatisfied with any member of TIME Team attending a Service Location to perform any part of the Managed Services, or such a member of TIME Team is found to be intoxicated, unruly, rude or have acted in a manner which is unbecoming whilst at the Service Location, the Customer will give written notice to TIME of such dissatisfaction and the specific reasons for such dissatisfaction. TIME will have seven (7) days from the receipt of such notice in which to remedy such problem to the reasonable satisfaction of Customer. If, after TIME's attempt at remedying the situation, Customer continues to be dissatisfied with the member of the TIME Team in question, then TIME will promptly replace that member of the TIME Team.

PART C – FAULT MANAGEMENT

10. SERVICE INTERRUPTION

10.1 **Service Interruption/Fault:** TIME does not warrant that the Managed Service is error-free, without interruption or fault. The Customer acknowledges and agrees that the performance of the Managed Services by TIME may be affected, impeded, interrupted or suspended by:

10.1.1 Customer's actions, inactions or lack of cooperation;

10.1.2 The inability of TIME to gain access to the Service Location in a timely manner;

10.1.3 The acts or omissions of third parties, including suppliers, contractors or providers engaged by Customer;

10.1.4 Non-payment or late payment of the invoices by TIME, including persistently paying invoices issued by TIME late;

10.1.5 Occurrence of a Force Majeure Event that affects the Managed Service and/or the Eligible Service;

10.1.6 Damage, loss or destruction of any of the MSE;

10.1.7 Request by you to suspend the Qualifying Service for any reason whatsoever;

10.1.8 Fault, interruption or disruption of the network or equipment of third party service providers;

10.1.9 Disconnection and/or reconnection of the Access Line(s), suspension or interruption of the Service pursuant to the General Terms and/or the terms in this Service Schedule, including non-payment of any Charges;

10.1.10 Power failure or disconnection of power supply either temporarily or otherwise;

10.1.11 Stolen telecommunication cables and/or fibre cuts that affect the Qualifying Service; and/or

10.1.12 Emergency maintenance and repair to the TIME Network that affects the Managed Service.

notwithstanding anything to the contrary in the General Terms.

10.2 Incident Reporting, Measurement and Closure:

10.2.1 **Incident Opening:** If the Customer experiences any interruptions or faults to the Managed Service, the Customer shall report the incident to the Service Desk. All such reported incidents results in the registration and opening of a trouble ticket with a reference number or identifier, and TIME will advise Customer of.

10.2.2 **Incident Closure:** TIME will inform Customer when it believes the incident is cleared, and subject to sub-paragraph (c) below, will close the trouble ticket when either Customer confirms that the Incident is cleared within twenty four (24) hours after being informed by TIME or TIME has closed the trouble ticket after unsuccessful attempts to contact Customer, by reasonable means, in relation to the Incident and Customer has not responded within twenty four (24) hours following TIME's attempt.

10.3 Attendance to Incidents Reported. TIME will restore the Managed Service reported by the Customer as quickly as possible, and in doing so may attend the Service Location to carry out necessary restoration work.

10.4 If:

10.4.1 Customer, confirms that the incident is not cleared within twenty four (24) hours after being informed that the incident is cleared, the trouble ticket will remain open, and TIME will continue to work to resolve the incident.

10.4.2 the incident is caused or contributed by the Customer, its servants, agents, invitees or any third party that gains access to the Service Location or the MSE, then the resolution of the incident shall be subject to Customer paying the costs incurred by TIME to trouble shoot and resolve the incident.

PART D – CHARGES

11. CHARGES. In addition to the Charges as defined in the General Terms and as specified in the Service Order, the following are applicable in respect of this Service Schedule.

11.1 Recurring Charges

11.1.1 **MRC**. Throughout the Initial Service Term, Customer will pay the MRC invoiced by TIME, including all applicable GST and other taxes, duties or charges as may be imposed by a governmental authority as a result of, in connection with or arising out of the provision of the Managed Services, other than income taxes that TIME is to pay.

11.1.2 **MRC on Renewal.** Clause 6.9 of the General Terms shall be applicable to Service types listed in this Service Schedule only.

11.2 Deposits: Unless waived by TIME, Customer shall pay TIME a deposit, the amount of which is specified in the Service Order, and if none is specified then no deposit is required to be paid.

11.3 Cancellation Costs: Wherever stated in this Service Schedule that the Customer is to pay Cancellation Costs, such Cancellation Costs shall be equal to the aggregate of the following items:

11.3.1 any Charges waived by TIME previously;

11.3.2 the price of the MSE that was delivered and installed by TIME as part of the provision the MSE at the Service Locations;

11.3.3 if the type of Managed Service is Wireless IPVPN, then charges imposed by third party service providers to TIME for TIME to provide this type of Managed Service only;

11.3.4 all incidental costs and expenses incurred by TIME in carrying out preparatory work to provision the Managed Service.

11.4 Termination Charges: Wherever stated in this Service Schedule that the Customer is to pay Termination Charges, as compensation to TIME, such Termination Charges shall be equal to the aggregate of the following items:

11.4.1 any Charges previously waived by TIME where the premature termination occurs during the Initial Service Term only;

11.4.2 the price of the MSE that was delivered and installed by TIME at the Service Locations;

11.4.3 if the type of Managed Service is Wireless IPVPN, then charges imposed by third party service providers to TIME for TIME to provide this type of Managed Service only;

11.4.4 any charges imposed by third party suppliers or contractors to TIME (if any) in order for TIME to provide the Managed Service;

11.4.5 as compensation for early termination of the Managed Service during either the Initial Service Term or Renewed Service Term, a sum equal to fifty per cent (50%) of the MRC for the remaining months of either the Initial Service Term or Renewed Service Term (as the case may be), which is a genuine pre-estimate of damages.

11.5 Invoice Disputes. In addition to Clause 6.8 General Terms, if the Parties are unable to resolve the dispute as to an invoice, then (a) Customer agrees that a disputed invoice pending resolution shall not be a valid ground to withhold payment of future invoices issued by TIME for the Services; (b)

TIME shall not suspend the Service to the Customer on the ground that the invoice remains outstanding, and (c) either Party may refer the dispute to arbitration.

PART E - MISCELLANEOUS

12. TERMINATION

12.1 BY CUSTOMER

12.1.1 The Customer may, in addition to any right to terminate specified in General Terms, terminate the Managed Services if:

(a) the Customer intends to vacate a Service Location provided that prior notice to vacate is given to TIME according to Paragraph 3.3.1 of this Service Schedule;
(b) the persistent and regular failure of the Managed Service.

then the Customer shall notify TIME in writing and specifying the date of termination, whereupon Customer shall pay TIME the Balance Charges and any third-party charges that are due and payable by TIME in order to terminate the Managed Services, as invoiced by TIME but no Termination Charges are payable.

12.1.2 If TIME without reasonable cause or excuse fails, neglects or refuses to carry out or provide the Managed Service, then the Customer may issue a notice to TIME requiring TIME to do so, and if TIME does not do so within the TIME specified in the notice (which must be a reasonable TIME), the Customer may terminate this Agreement, and neither the Balance Charges nor Termination Charges are payable by Customer.

12.2 CROSS-TERMINATION

12.2.1 If a Qualifying Service is terminated either by the Customer or TIME, then the Managed Service is automatically terminated on the same day as the date of termination of the Qualifying Service and:

(a) if the termination is by the Customer due to the fault of TIME, pursuant to Clause 8.1 or 8.3 of the General Terms, then only the Balance Charges is payable by Customer in order to transfer the ownership of the MSE to the Customer; or
(b) if the termination is by TIME due to the fault of the Customer, pursuant to Clause 8.4 or 8.3 of the General Terms, then the Balance Charges and Termination Charges are payable by Customer, and TIME may invoice the Customer accordingly.

12.2.2 Notwithstanding anything to the contrary in this Service Schedule, General Terms or any other service schedule, any termination of the Managed Service does not automatically terminate the Qualifying Service nor affect the continued provision of the Qualifying Service or the Parties obligations thereof.

12.3 BY TIME

12.3.1 Without prejudice to TIME's right to terminate pursuant to Clause 8.3 or 8.4 of the General Terms, TIME may terminate the Managed Services if:

(a) the MSE is damaged, destroyed, stolen or vandalised whilst under the control of the Customer;
(b) TIME has reason to believe that the Customer' has used the Managed Service in a manner contrary to Applicable Law and/or public policy.

and the Customer shall pay the Termination Charges and the Balance Charges to TIME

12.4 If the Agreement is terminated due to a Force Majeure Event pursuant to Clause 8.5 General Terms, then only the Balance Charges shall be payable by Customer in order to transfer the ownership of the MSE to Customer, and neither Party shall be liable to the other Party for any losses, damages or expenses suffered.

12.5 Upon termination, TIME shall immediately cease the provision of the Managed Services to Customer and the Customer shall immediately cease the use of the Managed Service.

[The remaining of this page is intentionally left blank]