MASTER SERVICES AGREEMENT
SERVICE SCHEDULE

SERVICE CREDITS FOR MULTI-BU SUPPORT SERVICES

This Service Schedule is attached to Order ref no. _____ issued pursuant to a Master Services Agreement no. _____ dated _____ entered into between Adventus Singapore Pte. Ltd. (the "**Supplier**") and _____(the "**Customer**") (this "**Service Schedule**").

WHEREAS

A. The Customer requires and the Supplier agrees to provide one or more suitably qualified engineers to render services to the Customer, more particularly described in **ANNEX B**; and

B. The Supplier shall be obliged to provide the Services only where the Customer has available Service Credits with the Supplier.

NOW, THEREFORE, it is hereby agreed as follows:

1. Purpose

Subject to the terms and conditions set forth herein, the Supplier agrees to provide the engineer(s) to perform services and Customer agrees to accept the services rendered by the engineer(s) (the "**Services**"), more particularly described in **ANNEX B**.

2. Service Activation

2.1 The Customer shall follow the procedure set forth in **ANNEX A** when requesting for the Services.

2.2. The Supplier reserves the right to change the process if this would, in the opinion of the Supplier, lead to more expeditious and efficacious resolution of the problem encountered.

3. Selection of Engineers

3.1 The Supplier shall provide the engineer to perform the Services set forth in **ANNEX B**.

3.2 For the avoidance of doubt, the Supplier shall have full discretion to select one or more of its engineer(s) to perform the Services provided that any engineer selected by the Supplier shall have the requisite qualifications and experience to perform the Services.

3.3 The Customer acknowledges that the engineer shall only be required to perform the Services set forth in **ANNEX B**. No other services shall be provided or implied.

3.4 Under no circumstances shall the engineer be deemed or considered an engineer of the Customer when performing the Services and should not represented as such.

3.5 For the avoidance of doubt, the Customer is not entitled to insist upon a specific engineer to perform the Services and acknowledges that the Supplier is entitled to send any of its engineers to perform the Services as long as the engineer has the requisite qualifications and experience to perform the Services.

3.6 The Customer acknowledges that even if a particular engineer is specified in the Order Form, this specification only represents the Supplier's intent in good faith to utilize the specified engineer as at the time of the Order to fulfil the Supplier's obligations under this Agreement. The specification of a particular engineer does not amount to a contractual or binding commitment on the part of the Supplier to utilize only the specified engineer to perform the Services.

4. The Supplier's Responsibilities

4.1 The Supplier will ensure that the Engineer has the requisite qualifications and experiences to perform the Services.

4.2 The Supplier shall provide the Engineer with adequate resources and support to ensure the Engineer is able to perform the Services.

4.3 During the term of this Service Schedule, the Supplier warrants that the performance of the Services by the Engineer shall not contravene any prevailing laws or regulations.

5. Customer's Responsibilities

5.1 The Customer undertakes to the Supplier throughout the term of this Service Schedule:-

5.1.1 to require the Engineers to perform only the Services set forth in **ANNEX B**;

5.1.2 to grant to the Engineer such access and facilities as he may require in order to perform the Services including without limitation adequate working space, required storage, the necessary equipment and other required facilities;

5.1.3 to take all reasonable precautions to protect the health and safety of the Engineer while on the Customer's premises; and

5.1.4 shall notify the Supplier as soon as practicable in the event of any breach or misconduct on the part of the engineer so that the Supplier may take suitable steps to remedy this.

6. Fees and Expenses

6.1 Customer shall pay the Supplier by way of Service Credits only. For the avoidance of doubt, Service Credits shall be purchased in advance by the Customer.

6.2 The terms and conditions relating to the use of the Service Credits shall be as stated in the Order Form or in the Supplier's website.

7. Warranty and Default

7.1 The Supplier warrants and undertakes that:

7.1.1 All personnel selected as the engineer are suitably qualified and competent to carry out the Services required of the Supplier under this Service Schedule;

7.1.2 the Supplier shall carry out its obligations in conformity with the general acceptance industry standards of skill, care and diligence appropriate to the nature of the service rendered.

8. Force Majeure

If the whole or any part of the performance by either party of any of its obligations under this Service Schedule is prevented, hindered or delayed or otherwise made impracticable by reason of strikes, labour troubles, floods, fires, accidents, earthquakes, lighting strikes, riots, explosions, wars, warlike conditions, hostilities, acts of government, or other cause of like or different character beyond the control of either party, and either party shall be excused from such performance during the continuance of any such contingency and for so long as such contingency shall continue to prevent, hinder or delay such performance.

9. Indemnity

In addition to Clause 13 ("Indemnity") in the Master Services Agreement, the Customer shall fully indemnify and hold the Supplier harmless against any and all claims or losses suffered by the Supplier arising from the performance of its obligations under this Service Schedule unless such claim or loss would not have arisen except for the Supplier's own default.

10. Non-Solicitation

The Customer and its related parties shall not directly or indirectly during the term of this Service Schedule or within two (2) years after the date of expiry of this Service Schedule, employ or make any attempt to offer employment, or procure or assist any other party to employ, any of the Supplier's engineers for its own use or another's employ or benefit.

11. Duration

This Service Schedule shall be valid and in force for the period stated in the Order Form, subject to any renewals and extensions.

12. Limitation of Liability

Clause 12 of the Master Services Agreement shall apply. In addition, the following shall also apply:

UNDER NO CIRCUMSTANCES SHALL THE SUPPLIER BE LIABLE TO THE CUSTOMER FOR ANY CONSEQUENTIAL, INCIDENTAL OR SPECIAL DAMAGES, INCLUDING LOSS OF PROFITS, LOST DATA OR LOST GOODWILL HOWSOEVER CAUSED EVEN IF THE SUPPLIER HAS BEEN EXPRESSLY INFORMED OF THE SAME IN ADVANCE. THE SUPPLIER'S MAXIMUM LIABILITY IN ANY CLAIM ARISING OUT OF THIS AGREEMENT WILL NOT EXCEED THE AMOUNT WHICH THE CUSTOMER HAS PAID TO THE SUPPLIER FOR SERVICES UNDER THIS AGREEMENT. UNDER NO CIRCUMSTANCES SHALL THE SUPPLIER BE DEEMED TO ASSUME OR BE LIABLE FOR THE BUSINESS AND OPERATIONAL RISKS ASSOCIATED WITH THE CUSTOMER'S OWN BUSINESS ACTIVITIES.

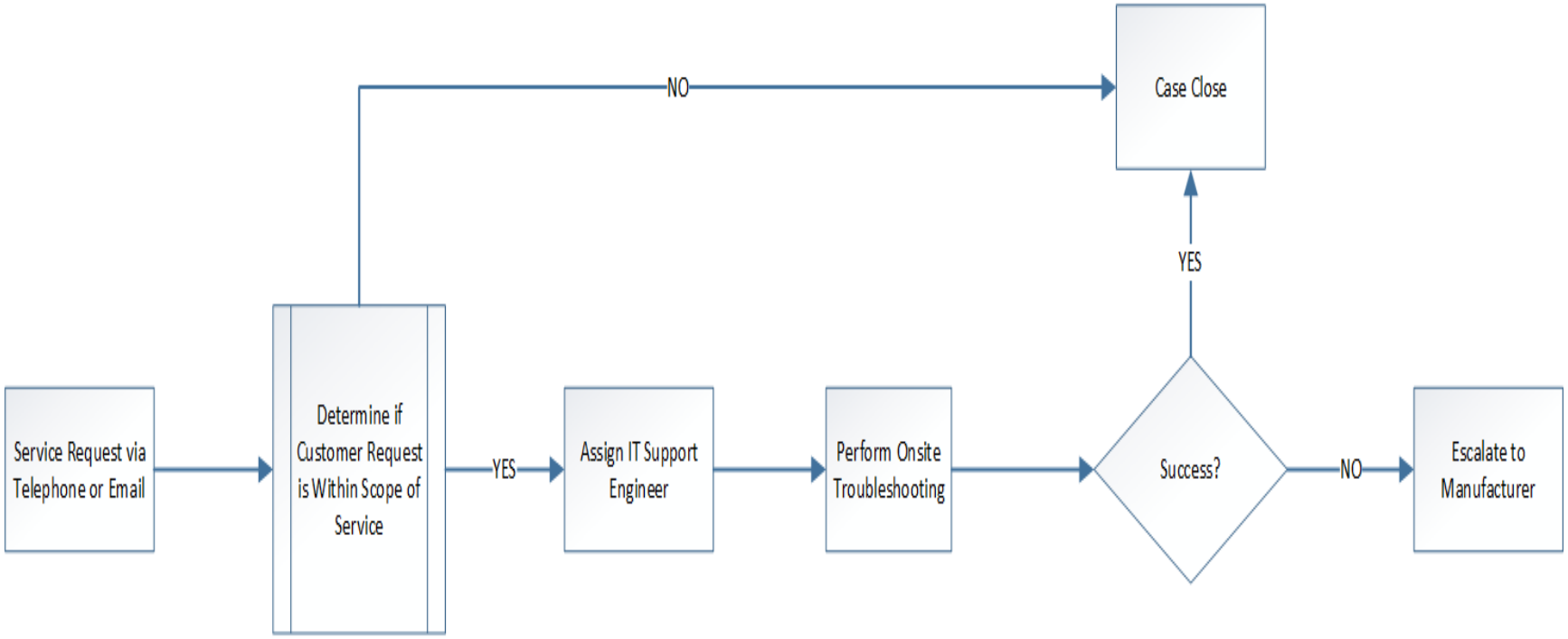
13. Entire Agreement

Together with the Master Services Agreement, this Service Schedule constitutes the entire agreement between the Supplier and Customer with respect to the provision of the Services and supersedes all prior negotiations, proposals, consents, correspondences, pledges, whether made orally or in writing. There are no understandings, representations or warranties of any kind except as expressly set forth herein. In the event of any conflict or inconsistency between the terms in this Service Schedule and the Master Services Agreement, the terms herein shall prevail in relation to the provision of the Services in this Agreement.

ANNEX A

SERVICE CREDIT FOR MULTI-BU SUPPORT SERVICES

Service Activation Process



Support Hotline Number: +65 61003301
Support Email Address: service@adventus.com

ANNEX B

SERVICE CREDIT FOR MULTI-BU SUPPORT SERVICES

Table 1: General Scope of Services which Engineer is able to perform:

Activities	Coverage
Overview	Preparation and Deployment of New IT Equipment
	End User Computing Equipment Health Check
	End User Computing Equipment Maintenance
	New Software Deployment and Software Update Rollout
	Decommission of End User IT Equipment
	Internal IT Document/System Updates
	IT Inventory Update/Maintenance
Routine Health Check	Perform Essential Application Check
	Providing Instructions for Uninstalling Unnecessary or Unused Software to Improve System Performance
	Keeping End User's Antivirus and Antimalware Software Up to Date
	Offering Guidance on Defragmentation and Disk Cleanup to Maintain Efficient Data Storage
	Check Event Viewer Log for any Signs of Abnormal Activities
	Check Time Synchronization between End Point and Domain Controller to Prevent Trust Relationship issue
	Check Outlook Email Log if any Errors or Warnings
	Guiding Users on Cleaning the Computer's Exterior and Peripherals to Prevent Dust Buildup
	Keep End Users Informed about Known Issues, Upcoming Updates, And Maintenance
Preventive Maintenance	Patch Management System to Ensure that Software Updates and Patches are Applied
	Apply Antivirus or Antimalware Software Updated
	Power Cycle to Sustained High CPU Usage
	Apply Critical Updates or Patches on Desktop or Laptops
	Management and Configuration of Printer
	Mapped Shared Drive Connection Issue Solution
Breakfix Support	Assisting Users in Diagnosing and Resolving Common Software Issues
	Troubleshoot Connection Issues or Peripheral Malfunctions
	Offering Remote Desktop Support to Diagnose and Troubleshoot Issues
	Provide Updates and Assist on Escalation to Internal IT Team
	Configurations Setting for Microsoft Systems
	Escalation to Manufacturer, Supplier, or External Vendor Regarding Faulty Hardware and/or Technical Issues that Cannot Be Resolved by First Level or Second Level
	Error and Troubleshooting: General Issue on Printer
	Error and Troubleshooting: Printer Output or Print Failure
	Error and Troubleshooting: Print Spooler
	Error and Troubleshooting: User Profile or Logon for Windows
	Error and Troubleshooting: Network Issue
	Error and Troubleshooting: Storage Issue
	Error and Troubleshooting: Server Issue (Excludes Applications and Database)
	Error and Troubleshooting: Virtual Machine Issue (Excludes Applications and Database)
	Error and Troubleshooting: Exchange Issue
Warranty Support	Check Equipment Warranty Status
	Escalate Technical Issue to Equipment Vendor
	Log Warranty Cases with Equipment Vendor
	Coordinate with Equipment Vendor for Onsite Repair
	Coordinate with Equipment Vendor for Onsite Equipment Loan Set
	Coordinate Logistics for Faulty Equipment Delivery and Collection
End User Services	Provide Advice for IT Incidents Successfully Logged Through The Helpdesk Over the Phone
	Remote Access into End User's Computer Device to Perform Diagnostics and Troubleshooting
	Software Installation
	Setting Configuration
	Troubleshoot End User's Desktop or Laptop Computer's Internet and Network Connectivity Issues
	Troubleshoot End User's Desktop or Laptop Computer that Cannot Boot Up
	Reformatting of End User's Desktop or Laptop Computer
External Vendor Coordination	Escalation to Manufacturer, Supplier or External Vendor Regarding Faulty Hardware
	Coordinate Hardware Repair Efforts of Manufacturer, Supplier or External Vendor
	Submit and Coordinate Warranty Claims

Note: The above scope represents the services which the Engineer is able to perform. The actual services rendered by the Engineer will depend on the specific requests made by the Customer.

Table 2: VAPT Scope of Services which Engineer is able to perform:

Activities	Coverage
Data Collection	**Inventory of Critical Assets:** • Identify and document all critical and regionally significant assets, including hardware, software, data, and network components. • Categorize assets based on their importance to business operations. **Topographic Data:** • Gather relevant geographical data to understand the physical layout and potential environmental risks. • Use GIS tools to map out critical infrastructure. **Scenario-Related Data:** • Collect data related to potential threat scenarios, such as historical incident data, threat intelligence reports, and industry-specific risks. • Analyze past security incidents and breaches to identify patterns and vulnerabilities.
Vulnerability Assessment	**Exposure Analysis:** • Evaluate the extent to which assets are exposed to identified threats. This includes network mapping, identifying open ports, and reviewing firewall configurations. • Use automated tools to scan for vulnerabilities in network devices, servers, and endpoints. **Sensitivity Analysis:** • Determine how sensitive assets are to these threats. This involves assessing the impact of potential vulnerabilities on business operations and data integrity. • Conduct risk assessments to prioritize vulnerabilities based on their potential impact.
Technical Assessment	**Network Scanning:** • Perform automated scans to identify vulnerabilities in network devices, servers, and endpoints. • Use tools like Nessus, OpenVAS, or Qualys to conduct comprehensive scans. **Penetration Testing:** • Conduct controlled attacks to exploit identified vulnerabilities and assess the effectiveness of existing security measures. • Simulate real-world attack scenarios to test the resilience of the network. **Configuration Review:** • Review the configuration of critical systems and applications to ensure they follow security best practices. • Check for misconfigurations, weak passwords, and outdated software. **Code Review:** • Analyze the source code of critical applications to identify security flaws and vulnerabilities. • Use static and dynamic analysis tools to detect coding errors and insecure practices.
Reporting	**Draft Report:** • Compile initial findings, including detailed descriptions of identified vulnerabilities, their potential impact, and recommended remediation steps. • Include visual aids such as maps, charts, and tables to illustrate key points. **Final Report:** • Present a comprehensive report with detailed findings, recommendations, and mitigation strategies. • Provide an executive summary for senior management and a detailed technical report for IT staff.
Remediation Support	**Action Plan Development:** • Develop a detailed action plan to address identified vulnerabilities, including timelines and responsible parties. • Prioritize remediation efforts based on the severity of vulnerabilities and their potential impact. **Implementation Assistance:** • Provide support to the organization in implementing recommended security measures. • Offer guidance on best practices and tools for vulnerability management. **Follow-Up Assessments:** • Conduct follow-up assessments to verify that vulnerabilities have been effectively mitigated and that security measures are functioning as intended. • Perform periodic vulnerability scans and penetration tests to ensure ongoing security.

Table 3: Cybersecurity Scope of Services which Engineer is able to perform:

Activities	Coverage
Initial Assessment	**Incident Confirmation:** • Verify the occurrence of the incident and gather initial details. • Identify the type and scope of the attack. **Communication Setup:** • Establish communication channels with the incident response team and key stakeholders. • Ensure secure communication to prevent further breaches.
Containment	**Immediate Containment:** • Isolate affected systems to prevent the spread of the attack. • Disconnect compromised devices from the network. **Long-Term Containment:** • Implement measures to maintain business operations while addressing the incident. • Apply patches, updates, and configuration changes to affected systems.
Investigation	**Data Collection:** • Gather logs, network traffic data, and other relevant information. • Preserve evidence for forensic analysis. **Root Cause Analysis:** • Identify the entry point and method used by the attackers. • Determine the extent of the compromise and affected systems. **Impact Assessment:** • Assess the damage and potential impact on business operations. • Identify any data that may have been accessed or stolen
Eradication	**Threat Removal:** • Remove malicious code, unauthorized access, and other threats from affected systems. • Clean and restore systems to their normal operational state. **System Hardening:** • Implement security measures to prevent future incidents. • Update and patch systems to close vulnerabilities.

Note: The above scope represents the services which the Engineer is able to perform. The actual services rendered by the Engineer will depend on the specific requests made by the Customer.

Table 4: Telephony Scope of Services which Engineer is able to perform:

Activities	Coverage
Overview	Diagnose or Localize Faults
	Repair, Restore Defective Parts and Perform any Remedial Work Required on Equipment
	Power or System Shut Down
	Holiday Greetings / Table Configuration
	Firmware or Service Packs Update
Remote MACD	Perform Remote MACD (Move, Add, Change, Delete of System Programmable features) **Add/Delete** • Activate/De-activate extension • Activate/De-active Voicemail or Reset Voicemail Password **Move/Change** • Change User Name Display • Swapping of phone from one location to another (must be analog-to-analog, or digital-to-digital) • Reprogramming of phone type (only for change of digital or IP Phone model) **Features Changes** • Speed Dial of system and user • Auto-Dial – Memory Button for storing a frequently dialed number • Call Transfer • Activate Call Forward (when no answer or busy) • Call Picky – To answer calls within user's pickup group • Call Park – to park calls away from desk and pick up from other extensions • Last number re-dial • Ring Again or Auto Call-Back for internal extensions • Message light • Conference – To set up conversation with up to 6 internal/external parties (include user) • Boss/Secretary • IDD Pin Codes • Call Barring – Restriction on overseas (IDD/STD)/External Calls **System Setting** • Set System Date/Time (Only for PABXs that allow remote change or do not need reboot after the change)
Preventive Maintenance	Backup Configuration Date
	Backup for OS, Security and Server and system Files data
	Screen capture on configure server (for IP setting on the media servers)
	Screen capture on the license file
	Visual check on the Hardware
	Verify the room condition (temperature and cleanliness)
Fault Recovery	**Major Fault** • External calls cannot be made/received • Extension of key appointment holders in customer organization is down • 50% or more of the extensions are down • 50% or more of the users' voicemail are down • Report cannot be generated from BCMS/CMS • Announcement system is down • 50% or more of Operator consoles are down • Conference bridge is down **Minor Fault** • All faults that are not classified as major fault **Set System Date/Time** *(Only for PABXs that allow remote change or do not need reboot after the change)*

Note: The above scope represents the services which the Engineer is able to perform. The actual services rendered by the Engineer will depend on the specific requests made by the Customer.

Table 5: Security System Scope of Services which Engineer is able to perform:

Type of System	Coverage
CCTV	Check the camera positions and ensure the cameras are focused and adjusted properly
	Check that camera view can capture the scene and can see the perimeter of the view clearly
	Clean any dust or marks off the camera lens and wipe down the camera casing if it is causing any blurry images when viewed through the CCTV monitor
	Check that camera's functions, such as zoom and pan are working correctly
	Advise the client accordingly if there is a need to increase the CCTV camera coverage or relocate the camera position
	Check that the cameras are securely attached to the wall / ceiling
	Ensure the camera locations are in line with the Floor plan layout
	Check the NVR settings and configurations to ensure that there is no default settings
	Check the HDD of the NVR and ensure is working
	Check that the monitors are showing a clear picture and that the brightness and settings are correctly adjusted
	Check that all switches and individual equipment are functioning fully
	Check that equipment are in good condition and that there are no weak connections
	Check that the correct time and date stamp is set
Access Control	Check the Central server or PC located onsite and ensure is operating
	Check that hosted solution on the cloud for Data storage is operating, if any
	If the access control is deployed over multiple sites, Check whether the LAN or Wireless Protocol is working or connected to the device
	Check the EML Lock, Release button, Break-glass and the Access Control device are operatively functioning accordingly
	Check the system records on the entry record of the personnel
	Check that number and type of readers are in accordance with the specification and any amendment, if any
	Guide the client for Programming & Training on the application of the Access Control device, if required.
	Check that Power supply unit is working and functioning
	Check to ensure Reader timings are as specified

Note: The above scope represents the services which the Engineer is able to perform. The actual services rendered by the Engineer will depend on the specific requests made by the Customer.