IT SYSTEM MAINTENANCE AND SERVICE LEVEL AGREEMENT FOR CORE FINANCIAL SYSTEMS

This Agreement is made and entered into as of 30 October 2025 (the "Effective Date").

BETWEEN:

ABC Agency (the "Authority"), a Governance Agency with offices at 1800 Commerce Plaza, Sunrise Street, Singapore 123456.

AND

TECHSERVE GLOBAL SOLUTIONS (the "Service Provider"), a company with offices at 77 Technology Drive, Innovation Tower, Level 22, Singapore 654321.

ARTICLE 1: SCOPE OF SERVICES

1.1 Covered Systems: The Service Provider shall provide comprehensive maintenance and support services for the Authority's Core Financial Systems (General Ledger and Accounts Payable Modules), including the associated 3 Production Servers and the primary network switching infrastructure identified in Schedule A.

1.2 Exclusions: This contract specifically excludes support for:

(a) End-user hardware (laptops, desktops, printers).

(b) Third-party vendor licensing issues.

(c) System upgrades requiring a major license revision.

ARTICLE 2: SUPPLIER OBLIGATIONS & DELIVERABLES

2.1 Maintenance Performance (Core Obligations): The Service Provider's primary obligations include, but are not limited to:

(a) Bug Fixing: The Service Provider shall fix any confirmed Software bugs or errors identified within the resolution times defined in the SLA (Article 3).

(b) Proactive Monitoring: Continuous, 24x7 monitoring of the Covered Systems to detect, prevent, and mitigate potential service disruptions.

(c) User Query Handling: The Service Provider shall serve as the Tier 2 escalation point and shall handle all user queries escalated from the Customer’s internal Tier 1 help desk.

2.2 Reporting and Governance (Deliverables): The Service Provider shall produce and submit the following documents/reports:

(a) Monthly Service Review Meetings: The Service Provider shall attend a monthly meeting with the Customer's ICT Manager to review performance, incidents, and changes.

(b) Monthly Performance Report: A comprehensive Monthly Performance Report must be submitted within 5 business days of the month end, detailing:

Uptime statistics for each Covered System.

A breakdown of all incidents by Priority Level (P1, P2, P3).

The SLA compliance percentage for Response and Resolution times.

(c) Incident Root Cause Analysis (RCA): An RCA document shall be submitted for every P1 incident within 7 days of the incident's resolution.

ARTICLE 3: SERVICE LEVEL AGREEMENT (SLA)

The Service Provider guarantees performance to the following measurable Service Levels:

3.1 System Availability (Uptime):

The Uptime for the Covered Systems shall be 99.9% per calendar month, excluding scheduled maintenance windows defined in Section 4.1.

3.2 Incident Response and Resolution Targets:

Priority Level	**Definition (Impact)**	**Required Response Time (Acknowledgement)**	**Required Resolution Time (Service Restoration)**
P1	System Down/Critical Failure. Total loss of service or major business function.	15 minutes	4 hours
P2	Major Degradation. Partial loss of service or severe impact on multiple users.	30 minutes	8 business hours
P3	Minor Degradation. Single-user issue or non-critical functionality.	1 hour	48 business hours

3.3 Patching Cycle: All critical security patches must be applied to the Covered Systems within 14 days of the vendor's official release date.

ARTICLE 4: LIQUIDATED DAMAGES (LD) & PENALTIES

The parties agree that damages resulting from a breach of the SLA are difficult to quantify; therefore, the following Liquidated Damages shall apply:

4.1 Uptime Breach Penalty:

If the actual Uptime for a month is below 99.9%, the Customer shall assess a penalty of 1.5% of the monthly fee for every 0.1% shortfall (or fraction thereof).

4.2 P1 Resolution Time Breach:

A fixed penalty of $500.00 USD per breach will be assessed for every Priority 1 incident not resolved within the 4-hour target.

4.3 Total LD Cap:

The total Liquidated Damages payable by the Service Provider in any single calendar month shall not exceed 25% of the monthly fee for that month.

ARTICLE 5: TERM

5.1 Initial Term and Renewal

The initial term of this Agreement shall commence on the Effective Date and continue for a period of two (2) years (the "Initial Term"). Following the Initial Term, the Agreement shall automatically renew for successive one (1) year periods (each a "Renewal Term") unless either party provides written notice of its intention not to renew at least ninety (90) days prior to the expiration of the Initial Term or any subsequent Renewal Term.

ARTICLE 6: TERMINATION

6.1 Termination for Convenience (Notice Period)

Either party (the Authority or the Service Provider) may terminate this Agreement for convenience (without cause) by providing the other party with a minimum of sixty (60) days prior written notice. The termination shall be effective on the date specified in the notice.

6.2 Termination for Cause

Either party may terminate this Agreement immediately upon written notice if the other party:

(a) Commits a material breach of any term or condition of this Agreement (including, for the Service Provider, failure to meet the SLA targets that results in the total monthly Liquidated

Damages Cap being reached in two consecutive months), and fails to cure such breach within thirty (30) days after receiving written notice of the breach.

(b) Becomes insolvent, makes an assignment for the benefit of creditors, or files for bankruptcy.

6.3 Obligations Upon Termination

Upon the termination or expiration of this Agreement for any reason, the Service Provider shall:

(a) Immediately cease all service activities.

(b) Provide all reasonable cooperation to the Authority in transitioning the services to an alternative provider or to the Authority’s internal team.

(c) Return or securely destroy all of the Authority's Confidential Information and property within seven (7) days of the termination date.

ARTICLE 7: CONFIDENTIALITY AND DATA SECURITY

7.1 Definition: "Confidential Information" means all non-public information, including, but not limited to, financial data, business plans, system architecture, security policies, and any user data stored in the Covered Systems.

7.2 Non-Disclosure Obligation: The Service Provider shall:

(a) Maintain the Authority's Confidential Information in strict confidence and only use it for the purposes of performing services under this Agreement.

(b) Disclose Confidential Information only to employees or approved sub-contractors on a strict "need-to-know" basis.

7.3 Data Security and Compliance:

(a) The Service Provider warrants that it shall maintain appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all Authority data and the Covered Systems.

(b) The Service Provider shall comply with all applicable laws and regulations concerning data privacy and security.

7.4 Incident Response: The Service Provider shall notify the Authority immediately, but in no event later than twenty-four (24) hours, upon discovery of any suspected or actual security breach or unauthorized access to the Covered Systems or Authority data.

ARTICLE 8: GENERAL TERMS AND LIABILITY

8.1 Intellectual Property:

(a) All existing Intellectual Property (IP) owned by the Authority remains the exclusive property of the Authority.

(b) Any code, documentation, scripts, or modifications created by the Service Provider specifically for the Covered Systems during the term of this Agreement shall be deemed "Work for Hire" and shall become the exclusive property of the Authority upon creation.

8.2 Indemnification:

The Service Provider shall defend, indemnify, and hold harmless the Authority, its officers, and employees from and against any third-party claims, liabilities, costs, and expenses (including reasonable attorney's fees) arising out of or related to:

(a) Any claim that the Service Provider's tools or methodology infringe upon the intellectual property rights of a third party.

(b) The Service Provider’s gross negligence or willful misconduct in the performance of the services.

8.3 Limitation of Liability:

(a) Except for the obligations under Section 8.2 (Indemnification) or a breach of Article 7 (Confidentiality), the Service Provider's total aggregate liability for all claims arising out of this Agreement shall not exceed the total fees paid by the Authority to the Service Provider in the twelve (12) months preceding the event giving rise to the claim.

(b) Exclusion of Damages: In no event shall either party be liable for any indirect, incidental, consequential, special, or punitive damages (including, but not limited to, lost profits or business interruption), regardless of the form of action.

8.4 Force Majeure: Neither party shall be liable for any failure to perform its obligations (other than payment obligations) where such failure is caused by an event beyond its reasonable control, including but not limited to, acts of God, war, riot, fire, flood, or pandemic-related government action, provided the affected party uses reasonable efforts to mitigate the impact and provides prompt written notice.

8.5 Governing Law: This Agreement shall be governed by and construed in accordance with the laws of Singapore, without regard to its conflict of law principles.

Schedule A: Covered Systems and Infrastructure

This Schedule identifies the specific systems, servers, and primary network switching infrastructure for which the Service Provider (TECHSERVE GLOBAL SOLUTIONS) is required to provide comprehensive maintenance and support services under this Agreement.

1. Core Financial Application Modules

System Name	**Module**	**Version / Build**
Financial Suite	General Ledger (GL)	v5.12.0
Financial Suite	Accounts Payable (AP)	v5.12.0
Database	Core Application Database	SQL Server 2019 Enterprise

---

2. Production Servers (3 Total)

All servers listed below are physical and located at the Authority's Primary Data Center.

Asset ID	**Server Name**	**Function / Role**	**Operating System**	**Location/Rack**
ABC-FS-001	FS-PROD-APP01	Primary Application Server	Windows Server 2022	Rack B, U21
ABC-FS-002	FS-PROD-DB01	Core Database Server	Windows Server 2022	Rack B, U22
ABC-FS-003	FS-PROD-WEB01	Web/Interface Server	Windows Server 2019	Rack B, U23

---

3. Primary Network Switching Infrastructure

Support is limited to the functionality and configuration of the listed network devices that **directly service the 3 Production Servers**.

Asset ID	**Device Name**	**Type**	**Model / Series**	**Location**
ABC-NW-010	SW-CORE-RKB	Core Data Center Switch	Cisco Catalyst 9500	Rack B
ABC-NW-011	SW-ACCESS-RKB	Rack Access Switch	Cisco Catalyst 2960X	Rack B

---

4. Support Hours and Contacts

Item	Detail
Standard Business Hours	Monday to Friday, 8:00 AM to 5:00 PM (Local Time)
Out-of-Hours Support	24x7 for P1/P2 incidents only (per Article 3)
Authority ICT Manager	Mr Tan Ah Meng, tan_ah_meng@abc.gov.sg,91234567
Service Provider Escalation	Mr Lim Ah Ben, lim_ah_ben@techserve.com, 98765432

This Schedule clearly defines the boundaries of the service, particularly by limiting network support to devices that directly service the core financial systems and by explicitly listing the three production servers.