SATS Airport Services Pte Ltd ("**SATS**") (Co Reg. No. 198500561R) invites quotes for the following:

TENDER NO. CT2007J012
DESCRIPTION:
Tender for the Supply, Installation and Commissioning of Servers and Associated Software for SATS Airfreight Terminal 6 Inventory Control System Servers

TENDER CLOSING DATE AND TIME: 1 September 2020, 1200hrs Singapore Time

ENQUIRIES

If you have any enquiries on the tender, please contact:

Person(s) to contact		Mr Ernest Lim
Tel No(s)	:	+65 65413872
Email	:	Ernest_LimLA@sats.com.sg

TABLE OF CONTENTS

INSTRUCTIONS FOR VENDORS 6
ANNEX 1: VENDOR PROFILE MATRIX 12
ANNEX 2: TERMS AND CONDITIONS ON USAGE OF SATS IT RESOURCES 14
ANNEX 3: SERVICE LEVEL AGREEMENT DURING LEASE/WARRANTY PERIOD AND INFRASTRUCTURE MAINTENANCE SERVICES (AFTER WARRANTY PERIOD) 17
ANNEX 4: INFORMATION SECURITY REQUIREMENTS 22
ANNEX 5: INFRASTRUCTURE AND ARCHITECTURE STANDARDS 25
ANNEX 6: SCOPE OF WORK - DETAILED 27
ANNEX 7: GLOSSARY 33
ANNEX 8: PRICING TABLE 34
ANNEX 9: STANDARD CONTRACT 36

EXECUTIVE SUMMARY

1. ABOUT SATS

1.1 SATS is Asia's leading provider of gateway services and food solutions.

1.2 Our comprehensive Gateway Services encompass airfreight handling, passenger services, ramp handling, baggage handling, aviation security services, aircraft interior and exterior cleaning as well as cruise handling and terminal management. Our Food Solutions include airline catering, institutional and remote catering, aviation laundry as well as food distribution and logistics.

2. BACKGROUND

2.1 The material handling system at AFT (Air Freight Terminal) 6 is fully automated and managed by the AFT6 Inventory Control System (T6 ICS). The server hosting AFT6 ICS was upgraded in year 2008-9. The AFT6 ICS system runs a mixture of HP Unix and Windows servers with Oracle databases.

2.2 The current hardware support cannot be guaranteed beyond year 2020 due to non-production reasons (the server models had ceased production) and because spare/replacement parts are no longer available in the market.

2.3 AFT6 ICS is critical to Operations and it is not feasible to run the system without the requisite support. Hence, there is a need to replace the SATS AFT6 ICS (Inventory Control System) servers to ensure business continuity.

3. SCOPE OF WORK

3.1 There is a need for SATS to replace the obsolete hardware and software at SATS AFT6 for the following ICS (Inventory Control System) Servers:

(a) ULD Control System (UCS)
(b) Maintenance Diagnostic System (MDS)
(c) Network Domain Controller (NDS)
(d) ICS Database Server (ICS)

3.2 The hardware support for the current system will be a problem due to spares availability.

3.3 Vendors are to quote for the following:

(a) Server Hardware and Software to replace the existing obsolete components
(b) Hardware architecture to support SATS' availability requirements
(c) Implementation and set up of the new servers
(d) Maintenance and support of the new servers
(e) Finance / Leasing arrangement for the servers/software over 5 years.

3.4 The response should demonstrate the ability of current and future products and/or services available. This should include those, which will be provided by partner Vendor(s), in order to meet the requirements within the RFP.

3.5 Business Objectives

- To ensure the smooth running of the T6 ICS system

- To upkeep the current availability and performance standards of the T6 ICS System

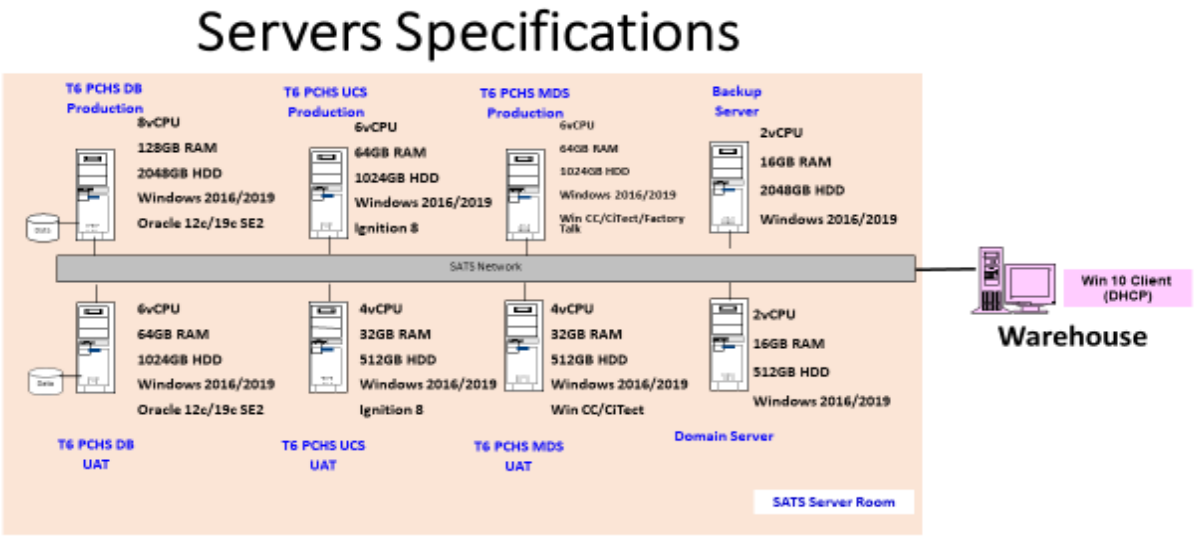
3.6 Financing

Vendor is to propose the following financing arrangements:

- Monthly or Quarterly leasing cost for hardware and system software for 5 years.
- Buyout from lease to convert to full ownership at the end of the 5th year, and
- Leasing cost should also include services provided by the vendor to setup / configure, test and manage the network and servers.

3.7 Current Infrastructure

The servers are being housed at Airfreight Terminal 6 Server Room. The replacement servers will be housed there as well.



UCS Servers
UCS application is used for PLC Communication and updates. Two (2) servers are currently used for UCS application.

MDS Servers
MDS application stores the real-time information of equipment. It monitors the equipment status and indicates errors and alarms when they occur. The SCADA application is a graphic representation of the equipment. Two (2) servers are currently used for MDS application.

NDS Server
NDS is a file server. One (1) server is currently being used and is intended for connection to client terminals and pushing down of antivirus patches

ICS Server
The ICS server contains database of the location of ULDs, flight schedules and all tasks and data controlling the automation of the MHS equipment.

3.8 The Vendor is expected to take on full and singular responsibility for the successful implementation of the hardware and associated software (including but not limited to) effective project management, delivery, integration, installation, training, warranty and maintenance support.

3.9 In the submission of the proposal, Vendors are strongly encouraged to include all features and capabilities of their product/solution that would be deemed beneficial to SATS. The Vendors are also encouraged to propose alternative solutions to meet the requirements stated in this RFP. Optional items should be quoted for separately.

3.10 Responses must include a detailed description as to (including but not limited to) how the requirements will be met, a proposed timeline for delivery and installation.

INSTRUCTIONS FOR VENDORS

SECTION 1: DEFINITION OF TENDER DOCUMENTS

Tender Documents shall include items listed in the RFT as well as all other documents issued prior to and after the deadline for Submission of Tender (tender bid).

The Tender Documents and additional materials that may modify or interpret, including drawings and specifications, by additions, deletions, clarifications or corrections will become part of the Contract when executed.

All Tender documents and clarifications shall form an integral part of a Contract that is to be entered into between SATS and/or its subsidiaries. Until a Contract is executed, the Tender Documents and clarifications shall be binding on Vendors.

All Annexes listed within, which form part of this RFP, will be issued accordingly as stated below:

Annex 1	-	Vendor Profile Matrix
Annex 2	-	Terms and Conditions on Usage of SATS IT Resources
Annex 3	-	Service Level Agreement during lease/warranty and infrastructure maintenance (after warranty)
Annex 4	-	Information Security Requirements
Annex 5	-	Infrastructure and Architecture Standards
Annex 6	-	Scope of Work (Detailed)
Annex 7	-	Glossary
Annex 8	-	Pricing Table
Annex 9	-	Standard Contract (“Contract”)

SECTION 2: SCHEDULE OF EVENTS

EVENT	DATE
Tender Publication	24 July 2020
Questions from Vendors	27 July 2020 – 25 August 2020
SATS Responses to Questions	28 July 2020 – 27 August 2020
Tender Briefing	30 July 2020, 11 am Location: Cargo Admin Office 5th Floor Core K Airfreight Terminal 5 Singapore 819830 Point of Contact: Mr Ernest Lim at 65413872
Submission of Proposal	1 September 2020 12 Noon, Singapore Time
Vendor Presentations	7 September 2020 – 10 September 2020 10am to 12pm or 2pm to 4pm Airfreight Terminal 5 (AFT5), Core K, Level 5, Cargo Conference Room
Appointment of Vendor(s)	Expected to be 3-4 months after Submission of Proposal, Validity of quote should be 9 months

SECTION 3: PAYMENT TERMS

Part 1: Payment Terms/Scheme

1. Vendors will follow the Payment Terms/Scheme as stated below:

2. For all One-Time Services, the following payment milestones will apply: -

Upon signing of Formal Contract	10% of Tender Amount
Upon delivery of hardware or system software	25% of Tender Amount
Upon system ready for installation	20% of Tender amount
User Acceptance Tests (UAT)	25% of Tender Amount
Upon System Operational	15% of Tender Amount
Upon end of Warranty Period	5% of Tender Amount

3. Leasing Option
   Leasing Cost will begin after delivery and installation of hardware and system software and will be paid on monthly or quarterly basis.

4. SATS and/or its subsidiaries have the right to terminate the Contract signed between SATS and/or its subsidiaries and the Vendors at any time giving thirty (30) days prior written notice. Should this occur, SATS and/or its subsidiaries will pay for work rendered up to date of termination.

Part 2: Pricing

5. For work covered in this RFP, Vendors must submit a fixed fee proposal (provide price breakdown where possible) within the **Annex 8** (Pricing Table).

6. All prices should be quoted in Singapore Dollars (SGD).

7. Provide a validity period of twelve (12) months from the deadline for Submission of Proposal.

8. Vendors shall bear any withholding tax, if applicable.

9. SATS reserves the right to award the RFP in whole, part or not at all.

10. Lease for 5 years must be submitted (Lease period should include comprehensive maintenance)

SECTION 4: FORMAT OF SUBMISSION

Part 1: Vendor Profile Matrix

Enclose the completed **Annex 1** (Vendor Profile Matrix) in this part. Please note that it is not acceptable to reference the relevant sections to e.g. websites, financial reports etc. Kindly fill in the required details.

Any supporting information/documents shall be provided as attachments to the Vendor Profile Matrix.

Do note that incomplete information could lead to disqualification.

Part 2: Tender Forms

Enclose within:
1. Tender Notice: Annex 3: **Tender Submission Form**
2. Tender Notice: Annex 4: **IPT Declaration by Vendor/Contracting Party**

If the Vendor is a corporation, the Tender Submission Form must be signed by an authorized officer of the corporation and stamped with the name of the corporation. No alteration in the Tender Submission Form is allows.

For IPT Declaration by Vendor/Contracting Party, to comply with Chapter 9A of the Listing Manual of the Stock Exchange of Singapore – Interested Person Transactions (IPT), declare whether your company is affiliated with Temasek Holdings Pte Ltd (owned by the Government of Singapore) or any of its subsidiary/associated companies.

Part 3: Executive Summary

Summarise the salient points of your proposal in no more than two (2) pages. Briefly describe your proposal and how it will meet the requirements of the RFP.

Part 4: Proposed Solution

The proposal should reflect the full understanding of all sections within the RFP.

Proposal could include:

- Hardware specifications, configuration and sizing to meet performance and availability requirements
- Detailed explanation of how the proposed configuration will meet SATS' availability requirements.
- Product upgrade path (e.g. details on new functionality/features/architecture and expected date)
- Security implementation, if necessary
- Detailed Managed Services
- Project management process/methodology, deliverables (e.g. project status etc.) and schedule
- Project organization structure and profile of key project team members
- Quality management plan
- Risk list and mitigation plan

- Details on how and the process to provide warranty and maintenance/support to comply with the stipulated SLA (including composition of team, escalation process etc.)
- Other details on provision of various environment, testing methodology, testing tools to be used, training, transfer of knowledge/skill etc.

State:

- the required configuration of your proposed product,
- If proposed system is a package, Vendors should highlight the salient features and describe the functionalities/features that would meet the functional and technical requirements (e.g. basic, mandatory, optional, value added etc.)
- All assumptions and constraints explicitly

State the time frame and schedule, from initiation till completion, for delivery of each (where possible) of the requirements.

Hardware / System Software warranty will be for at least a 12-month period, commencing from the date of system operational launch.

Part 5: Prior Experience

Vendors must provide extensive details of a minimum of three (3) projects, which they have relevant experience in. These must be similar to the nature of this Tender.

Part 6: Compliance Table

Provide a complete point-by-point response in ALL sections and Annexes. Include any additional information you deemed necessary to support your proposal, explaining how the proposed system would handle each requirement.

Annex 1	-	Vendor Profile Matrix
Annex 2	-	Terms and Conditions on Usage of SATS IT Resources
Annex 3	-	Service Level Agreement during lease/warranty and infrastructure maintenance (after warranty)
Annex 4	-	Information Security Requirements
Annex 5	-	Infrastructure and Architecture Standards
Annex 6	-	Scope of Work (Detailed)
Annex 7	-	Glossary
Annex 8	-	Pricing Table
Annex 9	-	Standard Contract (“Contract”)

This complete point-by-point response shall be done in a form of a Compliance Table as shown below, for the following RFP documents:

Para. No.	SATS Requirements	Compliance	Remarks
E.g. 2.14	Award of Tender		
2.14.1	Any subcontractors or assigned Vendors shall be named with the Tender Submission. [SATS] reserve the right to reject subcontractors or assigned Vendors without giving reasons, where Vendors will have no right to make changes to the final price in terms of compensation and/or replacement.	Y	

Vendors should enter a “Y” (Yes) or “N” (No) to indicate if it complies with the RFP requirement as written.

Vendors who do not comply with an RFP requirement exactly as written must enter an “N” in the “Comply (Y/N)” column and propose changes to the original RFP Requirements to clearly indicate the changes to the original RFP Requirement.

** Compliance with the T & Cs of the Contract will mean no change to the wordings of the clauses stated therein.

Describe how other Vendors or Vendors products, if any, will be integrated into your solution processes.

Describe the approach, processes and methodologies that you will be using in the system you are proposing.

ANNEX 1: VENDOR PROFILE MATRIX

Please complete the Matrix briefly (URLs are not acceptable). Additional information can be given as an attachment and / or in the relevant parts of your tender proposal.

Category/Section	Description
Corporate Information	
Company's Name and Address	
Year of Incorporation	
Parent Company Name and Address (if any)	
Mission and Direction	
Core Competencies / Business	
Revenue for the 3 most current year-end periods	
Net Profit for the 3 most current year-end periods	
Technology / Business Partner	
Contact Person's Name, Job Title, email address, mobile & DID contact no., fax no.	
Attendees to Project Briefing (if applicable) A maximum of three (3) representatives are allowed to attend the project briefing. Each organisation being represented must submit the Non-Disclosure Agreement (NDA). List the attendees' name, job title, NRIC / Passport No., vehicle no. (if any) and organisation name	
Experience	
Relevant Project Experience - number of years - state the projects title (a brief description can be given as attachment)	
SATS Project Experience - state the projects title (a brief description can be given as attachment)	
Relevant Customer Reference - list three (3) references	
Product Features	
Product Overview	
Technology Platform	
Years in Market	
Estimated Market Share	
Resources	
Number of Staff Worldwide - Total - Technical (Consultant, Engineer, etc.)	

Category/Section	Description
- Post Implementation Support	
Number of Staff in Singapore - Total - Technical (Consultant, Engineer, etc.) - Post Implementation Support	
Information Security and Quality Assurance	
State whether your organisation has a series of documented Information Security policies and Quality Assurance policies. Existing Information Security policies (Yes / No) Existing Quality Assurance policies (Yes / No)	

ANNEX 2: TERMS AND CONDITIONS ON USAGE OF SATS IT RESOURCES

Unless the context otherwise requires, references in this Annex to SATS or SATS' network, systems and assets refers to SATS Airport Services Pte Ltd, its subsidiaries and associated companies (the " SATS Group") and the SATS Group's networks, systems and assets

Pursuant to _____ Agreement dated _____ ("Agreement") between _____ < *Company* > and SATS, this letter is to confirm your said engagement by SATS will be subject to the terms and conditions of the Non-Disclosure Agreement dated _____ signed between _____ < *Company* > and SATS, and the following terms and conditions (which is not exhaustive).

In the performance of the services set out in the Agreement and to any and all other IT resources that SATS may have in future, you are advised and you agree and undertake to strictly adhere to the following terms and conditions ("T&Cs"):

(A) GENERAL

1. You agree and shall:
   a. endeavour to strictly comply with SATS' security policies when using or accessing SATS' IT resources including but not limited to, e-mail, intranet, and applications.
   b. protect the confidentiality of the PIN(s) or password(s) assigned to him/her at all times, and ensure that the same is not revealed or disclosed in any manner whatsoever to any person or persons whomsoever, within SATS or outside.
   c. use the IT resources strictly for official company business only, and will be responsible to ensure that resources will be used for the purpose intended for.
   d. acquire, install and use licensed and authorised software by SATS only, and in a manner permitted by the license.
   e. be responsible for the data accessed, retrieved, changed, stored or transmitted through any of the company's IT resources.
   f. inform SATS(IT_SATS@sats.com.sg) as soon as possible if they suspect that there is an IT security breach or when they experience an IT security breach.
   g. return to SATS all documents, papers, memoranda, software, hardware and any other property that you obtained from or prepared for SATS during the course of your engagement in SATS. You further undertake not to retain or make a copy such material or any part thereof, nor will you reconstruct such material based upon any confidential information known to you during your engagement with SATS.

2. You shall under no circumstances:
   a. use SATS' IT resources for
   i. private purpose, social or any unlawful purposes such as, but not limited to, vice, gambling or other criminal purposes;
   ii. sending to or receiving from any person any messages which is offensive on moral, religious, communal or political grounds, or is abusive or of an indecent or menacing character;
   iii. making defamatory statements about any person, party or organisation;
   iv. circulating "chain letters" or spreading rumours;
   v. distributing third party copyright materials;
   vi. distributing trade secrets or sensitive corporate information which may cause damage to the organisation, financially or otherwise; or
   vii. persistently sending messages without reasonable cause or for causing any threat, harassment, annoyance, inconvenience or needless anxiety to any person whatever.

b. engage in system activities that may in any way, result in inconvenience to other users of the system, or compromise the security of SATS' systems and network. Any attempts to crash the system, introduce malicious codes including but not limited to viruses and Trojan horse, gain unauthorised access, sabotage other systems using account or resources on SATS' system and network, or any other malicious attempts that cause any form of system damage to SATS' systems and network are all acts deemed as violations of these T&Cs.
c. attempt to or break the security mechanism which has been installed on SATS' computer equipment.
d. gain access or attempt to gain access to any computer system, information or resources without authorisation by the owners or holders of the right to such systems, resources and/or information.
e. violate intellectual property rights to the information or resources available.
f. make any copy or copies of any program/software that has been installed on your computer other than for backup or archival purposes.
g. download to the desktop or server any software that is subject to distribution limits.
h. transmit or remove confidential systems, applications or information/data from SATS' premises without SATS' approval.
i. port or transmit any information or software (into or out of SATS' network) which contains:
i. a virus, worm or other harmful component;
ii. prohibited material as defined by the Broadcasting Act (Chapter 28).
j. attach any unauthorised computer equipment, e.g., modem, to SATS' PC/workstation.
k. connect to an external network using computer equipment, e.g., a modem, while your PC, notebook or similar computer equipment is logged onto the SATS network.
l. bring in to SATS' premises personal or <Company> computer equipment such as notebooks with the intention of connecting on to SATS' network, without prior authorisation by SATS. In the event such permission is granted, you shall:
    i. ensure that the notebook is free of malicious codes such as viruses, worms or other harmful components by installing the latest updated version of an acceptable anti-virus software with its latest signature file on the notebook. Anti-virus software from the following companies are acceptable: McAfee, Symantec, and Trend Micro.
    ii. undertake that you will not, under any circumstances, connect to an external network, e.g., through a modem, while you are logged on to the SATS network.

(B) MISUSE OF SATS IT RESOURCES

SATS' systems are subjected to audit and users should therefore not expect a right to privacy.

Any unauthorised access or attempted access may be an offence under the Computer Misuse Act Chapter 50A and/or any relevant applicable law within and outside Singapore.

[For employers only] You undertake that you will ensure that any personnel under your employment and all others under your employment, including any sub-contractors or agents, having access to any of the confidential information and documents or such matters are subject to the same obligations as set out in the abovementioned T&Cs.

[For employers only] SATS reserves the right to request the removal of any of your employee from the Project team forthwith and/or terminate the Agreement forthwith if you or any employee or subcontractors or agents commits a breach of or is in non-compliance with any provision of these T&Cs. Should SATS request the removal of such employee, you will

endeavour to procure a replacement. Any such replacement offered by you shall be subject to SATS' prior written consent, which consent shall not be unreasonably withheld.

I acknowledge and agree that any act or omission which in any way is in contravention with the terms and conditions set out herein is expressly prohibited by law, may result in civil and criminal penalties to which I will be liable.

[For employers only] I further agree that I will at my expense, indemnify, defend and hold harmless SATS from any claim brought or filed by a third party against SATS due to my aforesaid act or omission.

I undertake to pay a minimum penalty of S$10,000 to SATS if it is established that malicious code has been introduced into SATS' network or a security breach has occurred, arising from an infringement of these T&Cs. SATS also reserves the right to terminate the contract in the event of a serious security breach.

The terms set out are acceptable to me, and are hereby agreed to:

{PRIVATE}

_____

AUTHORISED SIGNATURE

NAME: _____

DESIGNATION: _____

COMPANY: _____

DATE: _____

ANNEX 3: SERVICE LEVEL AGREEMENT DURING LEASE/WARRANTY PERIOD AND INFRASTRUCTURE MAINTENANCE SERVICES (AFTER WARRANTY PERIOD)

1. MAINTENANCE SUPPORT & HELPDESK HOURS

a. To provide 24 hours x 7 days maintenance support and helpdesk to all users.

2. PROBLEM RESOLUTION CRITERIA

a. Problem response time: The time taken by the maintenance team to validate, confirm and acknowledge that it is a hardware problem.

b. Problem resolution time: The time taken by the maintenance team to fix the problem, produce a workaround or resolution plan.

3. INCIDEMENT MANAGEMENT

a. Vendors will need to propose the incident management process.

4 SUMMARY OF VENDOR'S RESPONSIBLITY

a. Vendor shall provide the Helpdesk number through which SATS will log all problems related to the System.

b. Vendor shall also set up proactive monitoring and alert tools for automatic notification of system failures.

c. Vendor shall work closely with Application vendor to troubleshoot and resolve the problem whenever a system outage occurs.

5 SERVICE LEVEL FOR WARRANTY PERIOD AND SYSTEM/APPLICATION/HARDWARE MAINTENANCE SERVICES

5.1 SEVERITY LEVEL TABLE

Severity Level	Application		User Base		Impact to business and Operations		Acceptable workaround		Response Time (The time when investigation will commence)		Resolution Time (To produce Workaround or Resolution)
	Critical	Non-Critical	Widespread	Localised	Major	Minor	Yes	No	Office Hours	Out of Office Hrs	
1	X		X		X			X	30 min	60 min	3 hours
2	NA			X	X			X	60 min	60 min	> 95% within 6 hours Residual within 24 hrs
		X	X		NA			X			
3	NA			X		X		X	4 hours	Next working day	> 95% within 3 working days Residual within 5 working days
4	NA			X		X	X		1 day	Next working day	> 95% within 10 working days Residual within 12 working days

1. SEVERITY LEVEL DEFINITIONS

Critical	**Applications/Functions that provide services to SATS's customers either directly or indirectly**
Non-Critical	**Applications/Functions that provide a support function to the organisation such as Finance, HR, Lotus Notes etc.**
Widespread	**The proportion of users impacted is high, relative to the total number of users of a particular application or environment.**
Localised	**The proportion of users impacted is low, relative to the total number of users of a particular application or environment, i.e. a single user, site or functional area may be affected but many using the same functionality are still able to continue with their work.**
Major	**Significant impact on revenue generation ability, customer servicing or flight handling resulting in severe revenue loss, many dissatisfied SATS customers or numerous flight delays, or if safety is compromised.**
Minor	**There is business impact, but not of a serious consequence. Possibility of revenue loss, however, likely to be recovered with follow up calls or customer return; SATS customer service may be impacted, however customers can be satisfied in the interim, occasional flight delays may be incurred, however, not wide spread. Safety is not compromised.**
Acceptable workaround	**An acceptable workaround should be immediately available to allow the business to conduct its operations with little or no obvious impact to SATS customer facing services, and an acceptable level of user inconvenience may be experienced. The workaround may be application based (i.e. transactions or functions available to complete the business task), or they may be manual or procedural alternatives to the (unavailable) application functionality.**

5.3 SERVICE CREDITS FOR NON-COMPLIANCE OF SERVICE LEVELS DURING WARRANTY PERIOD AND INFRASTRUCTURE MAINTENANCE SERVICES (AFTER WARRANTY PERIOD)

In the event of a Service Level default (where the Vendor is unable to meet the Service Level stipulated in Section 5.1 above), the Vendor will provide Service Credits (SCUs). The maximum SCUs for non-compliance during a particular month is as given below. SCUs are payable in the following month in which the Service Level default has occurred, i.e. If Service Level default occurred in Jan 05, the SCUs are to be paid in Feb 05. Should the Vendor's non-compliance persist, SATS reserves the right to exercise other remedies under Contract and/or General Law.

Severity Levels	**Service Credits for Non-Compliance of Service Levels**
Severity level 1	NA
Severity level 2	5
Severity level 2.5	3
Severity level 3	2
Severity level 4	1

The value of the SCUs will be calculated using the following formula:

Value per SCU = $\frac{\text{Sum x At Risk Amount x Allocation factor}}{\text{Maximum SCU}}$

Sum = Value of Contract (15% of the Contract Sum during Warranty Period or Annual AMS fees during AMS)

At Risk Amount = Maximum % to be distributed for non-compliance of Service Levels, which will be 15%

Allocation Factor = Multiplier factor for non-compliance, which will be 4

Maximum SCUs = Total SCUs in a particular period, which is 11 (as per table above) x no. of months (twelve (12) months during AMS)

The Vendor acknowledges and agrees that the Service Level Credits and the Vendor's obligations relating thereto shall not in any way limit SATS's rights and remedies at law or under this Annex or the Agreement nor shall the Service Level Credits be deemed or construed to be liquidated damages or a sole and exclusive remedy or in derogation of any other rights and remedies SATS has hereunder or under the Agreement.

6. SERVICE LEVEL AGREEMENT (SLA) FOR AVAILIABILITY REQUIREMENT

The SLA provided by hardware vendor to SATS with an Availability of 99.5 % or 99.99 % overall quarterly average uptime of the hardware infrastructure that has redundancy built in the architecture.

System Availability includes consideration of the following:
1. Restore time service level agreements
2. System errors or time outs.

System availability expectations are as follow:

Service Level/Activity	Service Level Targets
Availability	99.5% or 99.99 % for hardware availability.
Scheduled Outage Notification	At least 5 working days prior to the outage
Service Level Reporting	Monthly report on the 15th of the following month covering details of the system availability, outages and performance in terms of response time. Details of the report content will be finalized later.

The system availability is calculated as follows:

$$\% \text{ Availability} = \frac{\text{Agreed Service Time} - \text{Planned} - \text{Unplanned Downtime}}{\text{Agreed Service Time} - \text{Planned Downtime}} \times 100\%$$

Definitions

Operational Hours	Time frame the business would like the application/service to be available for use.
Agreed Maintenance Window (AMW)	Window agreed with vendors for regular maintenance
Agreed Service Time	Operational Hours – Agreed Maintenance Window
Planned Downtime	Agreed Downtime outside of the Agreed Maintenance Window
Total Downtime	Unplanned Downtime + Planned Downtime + AMW

For example:
Application X, a 24 x 7 IT Service requires a weekly 0.5 hour agreed maintenance window (i.e. planned down time) for maintenance.
Following the completion of the 1st weekly maintenance, an application software error occurs which results in 3 hours of unplanned downtime.

The Availability for the IT Service for 1 month reporting period is therefore based on the following:

.	Hours
AMW/PD	0.5 hrs per week
AST	24hrs x 30 days = 720 hrs
UD	3 hrs

$$\% \text{ Availability} = \frac{720 - (0.5*4) - 3}{720 - (0.5*4)} \times 100$$

$$= 99.58\%$$

ANNEX 4: INFORMATION SECURITY REQUIREMENTS

The Vendor is obligated to adhere to the rules and obligations specified in this. Unless the context otherwise requires, references in this Annex to SATS or SATS' network, systems and assets shall include SATS Airport Services Pte Ltd, its subsidiaries and associated companies (the "SATS Group") and the SATS Group's networks, systems and assets.

1.1 Undertake to ensure that all its personnel/ subcontractors/ agents are aware of their security responsibilities, and will comply with SATS security policies and standards.

1.2 Comply with the Information security policy, information security standard, IT security framework, Implementation standards, technical standards and procedures throughout the development process

1.3 Guarantee that it does not knowingly hire (current or former) hackers

1.4 Accountable and responsible for maintaining the confidentiality, integrity and availability of any SATS systems and/or data entrusted to them

1.5 Undertake to ensure that its IT environment is secure and that SATS' network or systems will not be compromised through the Vendor's IT environment

1.6 Guarantee there is adequate separation of SATS resources from its other customers

1.7 Software that, intentionally or otherwise, attempts to breach the security of SATS' systems shall not be knowingly installed

1.8 Handling of security incident:

1.8.1 Immediately report any security incident involving their systems, and/or SATS IT resources to SATS' Information Security Department (Computer Incident Response Team), and cooperate with the investigation when required by SATS.
1.8.2 Ensure availability of services is maintained and take responsibility for the security incident.
1.8.3 All logs should be centrally stored and secured for possible forensic use. These would include but not limited to server, router, database, intrusion detection system, firewall and application logs

1.9 Dedicated to disaster recovery (applicable to hosting services):
1.9.1 Availability of hot-site facilities
1.9.2 Annual performance of recovery tests
1.9.3 Back-up procedures in place.

1.10 Implements controls to ensure protection against malicious software.

1.11 Protection of assets, including:

1.11.1 Procedures to protect SATS assets, including information, hardware and software;
1.11.2 Procedures to determine whether any compromise of the assets has occurred;
1.11.3 Controls to ensure the return or destruction of information and assets at end of, or at an agreed point in time, during the contract; and
1.11.4 Restrictions on copying and disclosing information.

1.12 Limitation of access to SATS' business information to authorized personnel supporting SATS' systems, and access must be restricted to authorized areas and granted based on valid business need only.

1.12.1 Physical and logical access controls to be used to restrict and limit access;
1.12.2 Third parties will not be allowed to access SATS' network through the Vendor's network;
1.12.3 Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
1.12.4 An authorization process for user access and privileges; and
1.12.5 Maintenance of a list of individuals authorized to use the services being made available and what their rights and privileges are with respect to each use.
1.12.6 Access by the Vendor's personnel/subcontractors/agents to SATS systems must be reviewed periodically to ensure currency of those personnel/subcontractors/agents and their access rights and the Vendor must immediately notify SATS when access is not required.
1.12.7 Privileged account access must not be shared. All users requiring privilege access must have unique user IDs.
1.12.8 All privileged activities must be logged. The log files or audit trails must be protected to facilitate future audit and investigations. The retention period of logs or audit trails needs to comply with legal and regulatory requirements.

1.13 Responsibility with respect to legal matters including but not limited to the following:

1.13.1 Subject to the Computer Misuse Act Chapter 50A and/or any relevant law within and Singapore.
1.13.2 Data, patent, copyright and privacy protection legislation
1.13.3 Intellectual property rights and copyright assignment and protection of collaborative work as provided for in the project agreement.

1.14 Non-disclosure of information including but not limited to the following:

1.14.1 Discovery of any security weakness shall not be disclosed to third parties, and shall be reported to SATS immediately;
1.14.2 The Vendor shall not disclose to third parties, whether directly or indirectly, information regarding SATS' network, details of the applications or other information that they may have access to during the course of contract with SATS

Save as provided for in the project agreement.

1.15 Compliance with a specified process for change management.

1.16 Obtain approval and clearance from SATS before the Vendor appoints subcontractors to support SATS' scope of work defined in the contract.

1.17 Encrypt all confidential data or email transmitted between SATS and the Vendor.

1.18 Obtain prior written approval from SATS before using SATS project work as a reference by the Vendor.

1.19 Submit an annual audit report, certified by the Vendor's auditors, on the services provided to SATS.

2. SATS reserves the right to:

2.1 Audit contractual responsibilities or to have the audits carried out by a third party without any notice;

2.2 Monitor, and revoke, user activity;

2.3 Terminate the contract immediately due to the existence of inadequate controls and/or for security violation by the Vendor's personnel/ subcontractors/agents;

2.4 Subject the Vendor's personnel/ subcontractors/ agents to SATS' personnel security review process;

2.5 Know the Vendor's external connectivity to other networks, and how the segment to be used for SATS is protected.

2.6 Vendors providing payment related services to SATS must comply with the guidelines published by Payment Card Industry (PCI) Security Standards Council at https://www.pcisecuritystandards.org/ during the term of the Contract. The payment related services include activities that require the Vendor to store, process or transmit payment cardholder (e.g., credit card) data. The Payment Card Industry Data Security Standards ("PCI DSS") is a multifaceted security standard intended to protect payment cardholder data. The Vendor shall undertake the required validation procedures according to their Service Provider Level, and provide to SATS the equivalent reports that they are required to submit to the payment brands or acquiring banks based on their Service Provider Level. The Vendor shall indemnify SATS for any security breach resulting in loss or misuse of credit card data due to Vendor's non-compliance of PCI DSS.

ANNEX 5: INFRASTRUCTURE AND ARCHITECTURE STANDARDS

Vendor's system or solution must operate seamlessly within SATS OT/IT infrastructure environment which comprise, amongst other things, the following:

Server Environment

- Operating System
  - Red Hat Enterprise Linux or
  - Windows Server 2016 or later
- Internet facing web server:
- Application Server
  - Application Server
- Messaging Software:
- Web Content Management:
- Transactional Database
  - Oracle 12c or later

- Network and Security Services
  - File and Print Server: Windows
  - Reverse proxy for employees accessing intranet web-based application through internet
  - Site-to-site VPN for data exchange and production/development environment support
  - Single sign-on for web based applications

- Data Centre Operation
  - IT Service Management and System Management/Monitoring
  - Backup, File System Management and HA/Fault Tolerant

Hardware standards

- HP UNIX servers
- Intel-based servers

The Vendor may use the following information as a guide to the processor speeds if the proposed solution involves Unix or Intel Servers. The approximate minimum processor speeds may be assumed to be as follows:

Components

SATS has a list of components that work in the WebLogic Application Server. While designing the solution, vendor should re-use these components if they satisfy the requirements.

***Note:**
IFS SOFTWARE" refers to all items stated in **Annex 9** (Infrastructure and Architecture Standards).

The Vendor's responsibilities include:
(i) Unless otherwise directed by SATS, ensuring that the Software is supported by the IFS Software at the version (the "N" release level) stated in Annex 5.

(ii) As directed by SATS, also ensuring that the Software is supported by the release N-1 and earlier versions of the IFS Software for the longer of:

(a) The thirty-six (36) month period following version N's general public availability.

(b) The time the IFS Software vendor ceases to support such version.

(iii) Using commercially reasonable efforts to maintain the versions of Standard Infrastructure Software needed by the Delivered Solution that is no longer supported by the Standard Infrastructure Software vendor.

The costs of continuously upgrading the Software to be supported by the IFS Software at the version "N" or N-1, will borne by the Vendor.

ANNEX 6: SCOPE OF WORK - DETAILED

1. Fault Tolerance, Availability and Reliability

- The T6 ICS is a fully automated, 24 by 7 system, vendors are expected to recommend solutions based on both 99.5% and 99.99%.
- There should not be more than four (4) unplanned downtimes per year.
    - For 99.5% availability, each unplanned downtime cannot be more than eleven (11) hours.
    - For 99.99% availability, each unplanned downtime cannot be more than thirteen (13) minutes.
- There shall not be any data loss should a server or its critical component go down in mid-transaction.
- There shall not be any data and transactions loss at failover.

Vendor must ensure that the above availability requirements are met and include fallback plan if any hardware components fail.

The vendor's proposal shall include a write up on how this level of Fault Tolerance can be achieved. Vendor's proposal may include any additional hardware/software components required. The cost for such components shall be clearly itemized.

2. Hardware Specifications

This section provides the required servers to be replaced. The intention is to combine the application to one server with one fault tolerant backup.
Disaster recovery to be provided at minimum cost with recovery of system within 4 hours.
Inventory data accurateness is not critical at time of recovery. However, non real time data should be accurate.

2.1 Server Requirements

A total of two (2) server groups shall be supplied in rack enclosures, each complete with Monitor, Keyboard and Mouse.

The servers are to support the following functions:
- PCHS ULD Control System (UCS)
- PCHS Maintenance Diagnostic System (MDS)
- PCHS Network Domain Controller (NDS) & Application / System monitoring and backup
- PCHS ICS Server (ICS)

VM ware to be provided to run the different applications

Specifications

S/no	Application	Description of Server	Quantity
1	UCS/MDS/ICS/NDS	• Intel Xeon Processors • Pluggable Hard Disk • Raid Controller • Network Card • Full Redundancy option	2
4	Rack & Rack Accessories	• Universal Rack / Shock Rack • Sidepanel Kit	

		• Rack Grounding Kit • Rackmount Keyboard Monitor	
5	UPS		

3. Software Specifications

3.1 The following are the software to be provided:

S/No	Software
1	Windows 2016 Server – Vendor to propose exact version that will support the proposed Fault Tolerance / Availability configuration
2	a) Solution and software to sustain 99.5% availability and fault tolerance of MDS/ UCS/ICS applications b) Solution and software to sustain 99.99% availability and fault tolerance of MDS/UCS/ICS applications
3	McAfee – Anti Virus
4	Oracle Database for Windows 2019 Server – Vendor to propose exact version that will support their proposed solutions
5	System Backup Software (Optional)
6	System Monitoring software (Optional)

3.2 Vendor must install and configure system software, and test all installations and configurations.

3.3 Vendor to specify and quote for the number of software licenses required to meet the proposed configuration.

4. SCADA and Communication Drivers Installation

4.1 Vendor must assist to install SCADA and Communication Drivers, and test all installations and configurations together with the Application Vendor, ASTrio.

4.2 SCADA and Communication Drivers will be provided by SATS.

5. Migration / Implementation / Testing / Training

5.1 The Vendor must work together with software vendors to ensure that the migration and implementation of the application software to the new hardware is successful.

5.2 The Vendor must provide standard basic training to SATS and Application Vendor. That includes the sequence and steps of start-up and shutdown of system software like Oracle, SCADA, Communication Drivers and perform simple diagnostics on the servers. This will enable SATS or Application Vendor to re-start the servers if required.

6. Testing and Acceptance

6.1 All components / systems shall be tested after successful installation. Vendors shall make accurate records of all tests and shall furnish test certificates and schedule of the test

results in an approved form. One (1) copy of such record and each test certificate shall be submitted to SATS for review.

6.2 All tests shall be conducted in the presence of appointed representative from SATS to the satisfaction of SATS. Vendors shall supply all necessary servers, system software. Connections and skilled labour required for the tests to be carried out to the satisfaction of SATS, without separate changes to SATS.

6.3 Vendors must / shall work with all relevant 3rd party vendors for the integration testing to ensure the installed system is able to support the requirement stated within this RPF.

6.4 Acceptance of the service will be based on the 100% compliance to configuration requirements within the scope.

7. Warranty

7.1 Vendor shall guarantee that the items supplied and/or services performed conform to the order made and are suitable for the use for which it is intended and is free from any defects whatsoever.

7.2 All software licenses and hardware supplied shall have a warranty of at least twelve (12) months from the day of delivery acceptance. Vendor to specify the warranty provisions in their proposal.

8. Financing

8.1 SATS would like to lease the hardware for a period of five (5) years. Thereafter, SATS shall have the option either to refresh the hardware at a preferential rate or to buy out the lease at a nominal price to convert to full ownership

8.2 SATS would like the option to lease the software for a period of five (5) years. Thereafter, SATS shall have the option to buy out the lease at a nominal price to convert to full ownership.

8.3 SATS would like the option to pay the one-time installation and set up costs in instalments.

9. Deliverables

9.1 Vendors must clearly indicate the management and deployment of the various deliverables with a detailed project schedule and plan. The following are some of the key deliverables (including but not limited to):

S/No	Deliverables
1	Bill of Material or Checklist
2	Hardware Diagnostic Test Results
3	Problem reporting and escalation procedures formalised
4	System Administration
5	Start up and Shut down Procedures
6	Application Monitoring Scripts set up
7	Integration Test Results
8	Failover Test Results

9	Backup / Recovery Test Results
10	User Acceptance Test Results
11	Troubleshooting Procedures
12	Operations Instructions
13	Commissioning Documentations
14	Failover and Recovery Process
15	Performance Monitoring Procedures
16	Proper procedure for recovery of services in event of failure

9.2 All documentation (stated above or otherwise) remains property of SATS.

10. Facility Management (FM) Services

Vendor shall provide the following FM services to manage the various system components.

10.1 Call Management

- A single point of contact for all hardware and system software problem reporting.

10.2 Priority System Recovery

- Immediate connection to a business or technical recovery specialist.
- Direct connection to a Microsoft Support Specialist.
- 24x7 hardware and systems software support to meet stipulated SLA.

10.3 SLA

- Critical problem notification
- Dedicated parts inventory
- 24x7 phone-in software assistance
- Enhanced Escalation Management
- Adopt severity level 2 of SATS's incident management service level agreement

10.4 Monthly System Maintenance

- Perform checks on system logs and rectify problems.
- Perform regular fail-over tests.
- Perform regular shutdown of servers to remove any memory fragmentation.
- Perform clean-up of specific file systems.
- Perform on-line file system backups.
- Apply Operating System (OS) patches (on a half-yearly basis), if applicable, on all the servers.
- Provide a report at the end of each month detailing any hardware faults found and rectified.

10.5 System Administration and Problem Resolution

System Administration should comprise:

- Set up new hardware, and install and configure system software, and test all installation and configuration prior to releasing to the application vendors,
- Apply Operating System upgrades and patches,
- Harden all hardware servers and database with all required security patches, a copy of the hardening document will be provided,
- Modify set-up and configuration on database and other servers that are required to support SATS's operation,

- Install and upgrade hardware components such as memory, hard disks, tape drives, etc., if required,
- Conduct regular house-keeping tasks,
- Conduct regular system health checks, and
- Formalize with SATS on the Change Management Process upon approval of changes and others.

Vendor would assist to identify, isolate and resolve faults that occur in the hardware and systems software. If need to, the vendor would escalate the problems detected to the relevant application vendor(s), and SATS shall be kept informed of all faults detected and the status of the faults.

Vendor shall propose the reporting and escalation procedures for all types of problems in their submission. SATS should only communicate with a single point of contact appointed by the vendor.

The vendor(s) shall submit monthly performance reports to SATS.

10.6 System, Database and Application Proactive Monitoring

Operating System – Vendor to provide performance and fault management services that employ scalable manager/agent architecture to provide the most effective means to remotely monitor and control network, system and database resources, and to proactively respond to any issues that may have been detected.

Deliverables of the performance and fault management services shall comprise:

- Proactive monitoring of critical server system resources and network equipment to ascertain the general health as well as to detect faults and errors.
- Detection of threshold conditions and faults shall be channelled automatically to alert engineers assigned to troubleshoot the problem before the problem becomes critical. Internet and SMS gateway connectivities are not currently supported and vendor will need to provide the hardware/software components necessary to support their proposed alert mechanism. Phone lines are presently available within the server room.
- Proactive analysis and highlighting of possible bottlenecks as well as potential capacity issues should be reflected in the monthly reports. These reports should be made available to SATS on a regular basis.
- Formalizing the process to alert SATS.

The performance and fault management of servers shall be a non-stop operation (i.e. 24x7 hours a day, 7 days a week, whole year round), and some of the parameters that could be monitored are:

- File systems (e.g. amount of file system space used) and Operating System,
- Processes (e.g. existence or absence). The application vendor(s) shall work with the Infrastructure vendor on all the application processes that need to be monitored,
- Services,
- Memory load (e.g. percentage of memory currently being used),
- Processor (e.g. CPU utilization), and
- Network and communication infrastructure.

Database and Application - Vendor shall provide the following services for database and application monitoring:

- Proactive monitoring of whether a service is active or inactive,
- Proactive monitoring of critical resources to ascertain the general health as well as to detect faults and errors,
- Detection of threshold conditions and faults shall be channelled automatically to alert engineers assigned to troubleshoot the problem before the problem becomes critical.

Vendor will need to provide the hardware/software components necessary to support their proposed alert mechanism. VPN is not allowed. Phone lines are presently available within the server room.

- Proactive analysis and highlighting of possible bottlenecks as well as potential capacity issues should be reflected in the monthly reports. These reports should be made available to SATS on a regular basis.
- The operating hours are 24x7 hours a day, 7 days a week, whole year round.

10.7 Backup

Vendor shall work with the application vendor(s) to define the back-up frequency and policies.

Backup services shall cover:

- Backup process verification (i.e. job is successful or unsuccessful),
- Data restoration,
- Inserting necessary tapes/drives for restoration, and
- Initiating restore process.

10.8 Security Checks and Monitoring

Vendor shall ensure that all necessary security measures are implemented and regularly updated.

Security measures include:

- Hardening of security configuration of servers, including operating system and application configurations. Vendors must conform to SATS OS hardening policy.
- Updating of security patches as and when they are released for server and/or system application software.
- Supplying and installing anti-virus software on all servers deployed in both production and test environments, as well as keeping up-to-date the virus patterns.
- Ensuring all servers are in compliance with SATS security policies upon implementation.
- Configuring and setting up system logs for the purpose of incidents and problems investigations.
- Segregate and prevent the testing data from development environment from entering into the production environment.

10.9 Services

Vendor shall provide the following services for the infrastructure support.

a) Maintenance should cover:
   - Problem troubleshooting.
   - System software upgrade.
   - OS/anti-virus patches.

b) The following is a list of infrastructure support services that the vendor must comply with. However, if the vendor is not able to comply with a particular item, the vendor must indicate the reason(s) for non-compliance and propose alternate arrangements, if any.
   - Solve problems reported by users. The response and resolution times should be as per the stipulated Service Level Agreement (SLA).
   - Maintain a knowledge database of the list of problems and solutions for future use by SATS and its nominated vendors.
   - Provide preventive maintenance to reduce the number of failures, and to improve stability, reliability and availability of the system.

- Prepare and submit Service Level Agreement (SLA) compliance reports, and weekly and monthly status reports. Vendor shall highlight the types of reports that SATS can expect to receive.
- For new releases of firmware or software, Vendors shall conduct planning together with SATS staff. The planning shall examine benefits of new releases, its impact on all existing equipment and the effort required for the update. Vendors shall ensure that all the hardware shall operate properly after such updates.

c) Work with SATS and propose yearly plans to introduce improvements (where deemed necessary) to be made continuously throughout the life of the contract. The adoption of a life cycle approach to service provision is seen as key to the improvement of service quality. Vendors should explain its approach in this regard. The plans should be presented to SATS at the start of each calendar for review and approval.

d) Ensure accuracy of all deployed hardware and software. At no point in time should the hardware and software be declared as End of Life (EOL) or End of Support from the hardware and software supplier(s).

e) Upon expiry or termination of the Facility Management Module or Maintenance Contract, the Vendor must ensure that services rendered to-date will be handed over to SATS and/or other SATS appointed vendor(s) with proper documentations or procedures specified by SATS. In addition, the Vendor will be required to conduct briefing sessions, presentations, handover procedures and on-the-job training to SATS staff and/or SATS appointed vendors. This will be at no additional costs to SATS.

ANNEX 7: GLOSSARY

No.	ABBREVIATION	DESCRIPTION
1.	ICS	Inventory Control System
2.	LCS	Logistics Control System
3.	MDS	Maintenance and Diagnostic System
4.	NDS	Network Domain Controller
5.	PCHS	Pallet Container Handling System
6.	SATS	Singapore Airport Terminal Services
7.	SCU	Service Credit Unit
8.	SATS	SATS Limited
9.	SLA	Service Level Agreement
10.	UCS	ULD Control System
11.	MHS	Material Handling System
12.	AFT	Airfreight Terminal
13.	SCADA	System Control and Data Acquisition
14.	OS	Operating System

ANNEX 8: PRICING TABLE

Sno	Price Components	Qty	Unit Rate (SIN)	Total Rate (SIN)
1.	**Installation Cost (One Time)**			
1.1	Server installation & set-up			
1.2	Oracle installation & set-up			
1.5	Installation and set-up of other necessary software			
1.6	Others, please specify			
	Sub-Total			
OR				
1.	**Installation Cost (Leasing)**			
1.1	Server installation & set-up			
1.2	Oracle installation & set-up			
1.5	Installation and set-up of other necessary software			
1.6	Others, please specify			
	Sub-Total			
2	**Monthly/Quarterly Leasing (Hardware)**			
2.1	UCS/MDS/ICS/NDS Servers	2		
2.4	Server Rack to house the servers			
2.5	UPS			
2.6	Others, please specify			
	Sub-Total			
3	**Monthly Leasing Software**			
3.1	Windows 2016 Server			
3.2	Oracle Database for Windows 2016 Server - Software Update License and Support			
3.3a	Solution and software to sustain 99.5% availability and up time of MCS/UCS/ICS applications - 1st year support - 2nd year support - 3rd year support - 4th year support - 5th year support			
3.3b	Solution and software to sustain 99.99% availability and up time of MCS/UCS/ICS applications - 1st year support - 2nd year support - 3rd year support - 4th year support - 5th year support			
3.4	McAfee – Anti Virus			
3.5	System Backup Software (Optional)			
3.6	System Monitoring Software (Optional)			
3.7	Others, please specify			
	Sub-Total			

Sno	Price Components	Qty	Unit Rate (SIN)	Total Rate (SIN)
OR				
3	**One Time Software**			
3.1	Windows 2016 Server			
3.2	Oracle Database for Windows 2016 Server - Software Update License and Support			

3.3a	Solution and software to sustain 99.5% availability and up time of MCS/UCS/ICS applications - 1st year support - 2nd year support - 3rd year support - 4th year support - 5th year support			
3.3b	Solution and software to sustain 99.99% availability and up time of MCS and UCS applications - 1st year support - 2nd year support **- 3rd year support** - 4th year support - 5th year support			
3.4	McAfee – Anti Virus			
3.5	System Backup Software (Optional)			
3.6	System Monitoring Software (Optional)			
3.7	Others, please specify			
	Sub-Total			
4	**Facility Management (FM) Services (3 years with optional extension by two years)**			
4.1	Call Management			
4.2	Monthly cost for FM services			
4.3	Others, please specify			
	Sub-Total			
5	**Buy Out from Lease to convert to full ownership at the end of the 5th year**			
	Total (Items 1 to 5)			
	Sub-Total			
	Grand Total			

ANNEX 9: STANDARD CONTRACT

<<For Standard Contract, please refer to PDF document(s) that is attached in email sent along with this RFT.

The Award of Tender shall be subject to such additional terms and conditions as may be agreed upon between SATS and the Vendor in addition to the terms and conditions specified in this RFP.

Vendor shall complete point-by-point response in a form of a Compliance Table as shown below:

Para. No.	SATS Requirements	Compliance	Remarks
1	Definitions and Interpretation		
1.1	In this Agreement, unless the context otherwise requires: Acceptance Date means the date on which SATS accepts the System in accordance with Clause 6.	Y	

Vendors should enter a "Y" (Yes) or "N" (No) to indicate if it complies with the RFP requirement as written.

Vendors who do not comply with an RFP requirement exactly as written must enter an "N" in the "Comply (Y/N)" column and propose changes to the original RFP Requirements to clearly indicate the changes to the original RFP Requirement.

Note: Compliance with the T&Cs of the Contract will mean no change to the wordings of the clauses stated therein. Provide point-by-point response to each clause of Annex 9 (Standard Contract), in the table format shown in the figure above.