SATS TECHNOLOGY

Request for Proposal

Project Title:	Autonomous Guided Vehicle for SATS Food Services Pte Ltd
RFP Number:	CT2010J020
Co. Regn No.:	197201770G

Confidentiality:

Do note that this Request for Proposal (RFP) is the property of SATS Ltd. (SATS) and/or its subsidiaries.

Any reproduction of its contents (in whole or part) except for the preparation of the Tender must have prior written approval by the designated representatives of SATS Ltd. and/or its subsidiaries.

TABLE OF CONTENTS

INSTRUCTIONS FOR VENDORS

SECTION 1: DEFINITION OF TENDER DOCUMENTS

Tender Documents shall include items listed in the RFP as well as all other documents issued prior and after the deadline for Submission of Proposal (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 and Vendors. 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 3	-	Tender Application Form
Annex 4	-	IPT Declaration by Vendor/Contracting Party
Annex 5	-	Individual Non-Disclosure Agreement
Annex 6	-	Terms and Conditions on Usage of SATS IT Resources
Annex 7	-	Sample Banker's Guarantee
Annex 8	-	WSH Rules and Regulations
Annex 9.1	-	Service Level Agreement
Annex 9.2	-	Service Level Agreement - Incident Management
Annex 10	-	Information Security Requirements
Annex 11	-	Infrastructure and Architecture Standards
Annex 12	-	IT Operations Standards and Guidelines
Annex 13	-	SATS Coding Practices
Annex 14	-	Application Maintenance Services
Annex 15	-	Scope of Work (Detailed)
Annex 16	-	Pricing Table
Annex 17	-	Standard Contract ("Contract")
Appendix A (2)	-	Envelope Label for Tender Submission

SECTION 2: SCHEDULE OF EVENTS

EVENT	DATE
Tender Publication	4 Dec 2020
[1] Project Briefing	NIL. Vendor to write in to request, if deemed necessary.
Questions from Vendors	7 -17 Dec 2020
SATS's Responses to Questions	8 – 18 Dec 2020
[2] Submission of Proposal	28 Dec 2020 at 1200 Hours Singapore Time
Vendor Presentation (onsite at SATS Premises) - tentative	29 - 30 Dec 2020
Appointment of Vendor(s)	Shall not be more than three (3) months after Submission of Proposal

[1] Refer to 3.4 Project Briefing
[2] Refer to 3.5 Tender Submission

SECTION 3: TENDER PROCEDURES

3.1. Contact Person

If there is a need to seek clarifications, requests should be sent as an attachment in Microsoft Word document to:

Contact Person: Yee Sheen Chua
YeeSheen_Chua@sats.com.sg

Victor Ang
Victor_ang@sats.com.sg

CC: IT_Procurement@sats.com.sg

ALL communications between the vendors and SATS and its subsidiaries shall be through the above email address.

When submitting questions, the identity of the Vendors' representative must be clearly indicated. The email shall in such cases, follow the format as stated below:
(1) Name of vendor;
(2) Date of submission; and
(3) Document Number e.g. Vendor XXX, 06 Feb 2014, Document 1 of 1 etc…

As to clearly specify how many email(s) and attachment(s) constitute the full proposal. All questions must be sent to SATS and/or its subsidiaries before the deadline indicated in *Section 2: Schedule of Events*. SATS and/or its subsidiaries will respond to the questions in writing. All the questions and the corresponding responses prior to the Submission of Proposal date will be made known to all Vendors (where possible) without revealing the identity of the source of the questions.

If the solution includes a partnership of service providers, the Prime Vendor will be the sole party that communicates with SATS and/or its subsidiaries during the Tender process.

3.2. Project Briefing

Each Vendor is only allowed to send a maximum of three (3) representatives to attend the project briefing.

Attendees are required to exchange their NRIC or Passport for the Visitor Pass at the respective SATS location(s) stated in Section 2 of this document.

Do note that any changes to the attendees list must be submitted to SATS at least three (3) working days prior to the vendor briefing for security clearance.

3.3. Tender Submission (Submission of Proposal)

Three (03) sets of the Tender Submission, i.e. **One (01)** set of original and **two (2)** sets of copies, are required. For identification purposes, the cover of the Tender Submission (including the envelopes) MUST be clearly marked with either 'ORIGINAL' or 'COPY' and the ***tender reference number***.

The submission of **Annex 16** (Pricing Table) is to be separated from tender proposals, i.e. **One (01)** set original and **two (2)** sets of copies for **Annex 16** (Pricing Table) are not to be filed or bind together with the tender proposal and it shall be filed or bind as a different document. The cover of the Pricing Table MUST be clearly marked with either 'ORIGINAL' or 'COPY' and the tender reference number, put them in an envelope marked "***Pricing table of tender reference number XXXX***".

In addition, prepare **TWO (2)** sets of CDs containing the soft copy of your Tender Submission**.** Label the CDs with the ***tender reference number, project name*** and ***your organisation's name***; and put them in an envelope marked "***Softcopy of tender reference number XXXX***".

The Tender Submission, comprising the proposal(s) and CDs, should be submitted in sealed envelopes to:

Secretary, Tenders Committee
(Non-Foodstuff and Other Equipment)
C/O SATS Security Entrance Gate
SATS Inflight Catering Centre 1
20 Airport Boulevard
Singapore Changi Airport
Singapore 819659

Note: For identification purposes, the cover of the documents (including the envelope – please use the envelope label shown below) MUST be clearly marked with ‘TENDER FOR AUTONOMOUS GUIDED VEHICLE FOR SATS FOOD SERVICES PTE LTD’ and the tender reference number. Tenderers must have the documents deposited into the BLUE SATS Tender Box located at the above-mentioned location. Please use envelope label provided for under Appendix A (2).

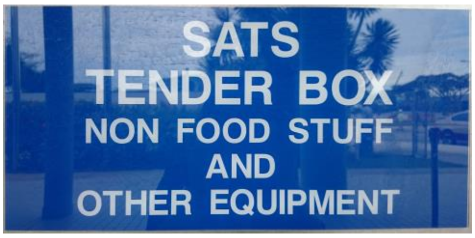


Figure 1: SATS Tender Box for Tender Proposals Submission

The time specified in *Section 2: Schedule of Events* under Submission of Proposal must be strictly adhered to.

All application documents must be signed and company-stamped before they are submitted.

In addition to the above, Overseas Vendors whom do not have an office presence in Singapore may submit via email – ensuring that the following steps mentioned must be fulfilled:

- Step 1 – Email quotation (in PDF file format) to the secured email account: CPTM_Procurement@sats.com.sg. Please DO NOT copy your submission to any SATS staff.
- Step 2 – The Original Tender submission of Proposal MUST be deposited into the BLUE SATS Tender Box within three (3) working days starting from the date and time of Submission of Proposal as stated in section 2: schedule of events. Otherwise, the Tender Submission will not be valid.

All application documents must be signed and company-stamped before they are submitted.

Late submissions will not be accepted.

3.4. Evaluation Criteria

The proposals will be evaluated based on the following factors (including but not limited):

- Overall value; i.e. cost versus benefit to SATS and/or its subsidiaries
- Point-by-point responses to the Scope of Work
- Completeness of your solution
- Ease of integration with current SATS and/or its subsidiaries systems
- Technical Expertise
- Prior Experience
- Any Value Added Services
- IT Security and Recovery controls
- Data access management

The evaluation process may include telephone calls to your referees (clients) to verify claims made by your company. Reference sites with the closest match to SATS's and/or its subsidiaries network will be preferred.

The short listed candidates may be asked to present their Tender Submission on-site at SATS and/or its subsidiaries. SATS and/or its subsidiaries will provide the necessary facilities for the presentation but all other expenses incurred by the Vendors in making the presentations will be borne by Vendors.

Agenda for the presentation will be sent beforehand to enable the short-listed vendors prepare for the vendor presentations. Vendors must adhere strictly to the agenda and time allocated to complete the vendor presentation.

3.5. Terms and Conditions of Tender

The responses (including clarifications) to this RFP are expected to be included in the Contract should the Tender bid be successful.

3.5.1 General Conditions

SATS and its subsidiaries reserve the right to discontinue with the RFP process at any time and make no commitment, implied or otherwise, that the RFP will result in a business transaction with one (1) or more Vendors.

SATS and its subsidiaries are not under any obligation to pay Vendors for information received. This RFP does not commit SATS and its subsidiaries to pay for any costs incurred by Vendors in responding to this RFP, nor does it commit SATS and its subsidiaries to procure products and/or contract for services.

3.5.1 Terms of Application

Application of Tender by Vendors constitutes acceptance by Vendors of all terms and conditions printed on this form and all other attachments hereto.

Upon acceptance of the Tender Documents, Vendors undertake to submit their proposal by the allotted time unless the Vendor(s) declares in writing, prior to the Submission of Proposal date, their intention not to bid for the Tender.

Vendors shall undertake the preparation of their Tender Submission at their own cost including travel to Singapore, if any, during the Tender process.

3.5.2 Tender Amount

Numbers shall be stated in writing and in figures.

The pricing for the products to be supplied or services to be rendered shall be exclusive of any Goods and Service Tax ("GST"), i.e. prices quoted shall not include any GST component.

The amount tendered by the Vendor and filled in the space "TOTAL AMOUNT TENDERED" on the **Annex 3** (Tender Application Form) shall be the amount agreed to upon appointment of the successful Vendors. The amount shall not be varied in any way, unless mutually agreed in writing.

Unless otherwise provided in any supplement to these instructions, Vendors shall not modify their Tender Submission after the Submission of Proposal date. The price quoted shall be treated as the last price the Vendor is prepared to offer. Vendors should therefore quote their BEST and last price.

Notwithstanding the above, should a change in specifications occur after a Tender has been called and such change may have an effect on price, SATS and/or its subsidiaries may under such circumstances revise the price with the vendors.

Vendors may not amend their bid price during the Contract period. Any increase in costs of production or in any other aspect may not be passed on to SATS and/or its subsidiaries by way of an increase in the awarded price or a change in the products and/or services to be provided.

Without limitation all permits, licenses, royalties and fees whatsoever claimable by or payable to any person, firm or corporation or government or in connection with an invention or patent used or required to be used in connection with Vendors obligations under this Tender are for the account of Vendors and shall not be charged to SATS and/or its subsidiaries.

3.5.3 Vendors' Responsibility

Vendors shall undertake the preparation of their Tender Submission at their own cost including travel to Singapore, if any, during the Tender process. The Submission of Proposal represents that the Vendors have read and understood the Tender Documents.

Whenever possible, the appointed Vendor shall identify sources of government grants (i.e. funding) for SATS' consideration. In the event SATS is awarded a government's grant (i.e. funding) for this project, the appointed Vendor shall provide all necessary supporting documents, including but not limited to, technical, functional, and commercial documentation for the purpose of the funding. The appointed Vendor shall be required to comply with all terms and conditions of the government grant. The appointed Vendor shall be required to attend and prepare for ad hoc on-site reviews and audits arising in accordance to the government grant for this project.

3.5.4 SATS's Obligations to Vendors

SATS or its subsidiaries will assist Vendors whenever and wherever possible in determining local conditions and clarification of the Tender Documents.

SATS may reject any, part of, or all Tender Submission and waive any informality or irregularity in any Tender Submission received. No reason shall be given to any unsuccessful Vendors for not being awarded the Tender.

3.5.5 Compliance to Requirements, Standards and Guides

Vendors shall comply with all business and technical requirements, standards and guides specified in this RFP unless otherwise stated in accordance with *Section 4: Format of Proposal, Part 3: Proposed Solution*.

Vendors are to comply with industry best practices and standards associated with (including but not limited to):

- Project management
- Infrastructure design
- Software development
- Infrastructure operations
- Information security

3.5.6 Acceptance of Tender

SATS and/or its subsidiaries shall not be bound to accept the lowest of any Tender Submission nor is it liable for any claim for whatever costs that may be incurred in the preparation of the Tender.

SATS and/or its subsidiaries reserve the right to accept and award the whole or part of the Tender Submission.

3.5.7 Notification of Vendors

All Vendors will be notified of the award as soon as approvals by the relevant committees have been given.

Vendors shall be notified in accordance to the timeline stated in Section 2: Schedule of Events (subjected to changes by SATS). Do note that Confidential Annexes shall only be released to shortlisted vendors.

3.5.8 Award of Tender

All sub-contractors or assigned Vendors shall be named within the proposal. SATS and/or its subsidiaries reserve the right to reject sub-contractors or assigned Vendors without giving reasons, whereby the Vendors will have no right to make changes to the final price in terms of compensation and/or replacement.

SATS and/or its subsidiaries may, at their discretion, award part of the products and/or services to other Vendors. Vendors are obliged to co-operate with each other including working with SATS's and/or its subsidiaries' vendors to deliver a solution that complies fully with the overall system (business and technical) specifications as specified in the RFP.

3.5.9 Communications

After the tender closing date, the vendors shall not communicate directly or indirectly with SATS or any of the employees of SATS in regard to the progress of the Tender (unless otherwise specifically stated within the Tender documents), other than through the official channel (refer to Section 3.1: Contact Person).

SATS shall communicate the results of the Tender to the vendors in writing.

The breach of this term and condition by the vendors, their employees or agents shall render the vendors to be disqualified from this Tender exercise or any future tender exercise.

3.5.10 Conformance with Agreed Specifications

All works must be carried out in accordance with the Tender Documents that have been agreed to by SATS and/or its subsidiaries and Vendors.

All title, ownership and other intellectual property rights in any software customization and related documentation created or otherwise developed pursuant to this Tender vest in SATS.

By submitting the Tender, Vendors agrees to assign to SATS any intellectual property rights that subsist in or arise from the deliverables of any software customization and related documentation created or otherwise developed pursuant to this Tender.

If vendors do not agree to the assignment, they must explicitly specify the reasons in the RFP submission, subjected to approval by SATS.

3.5.11 Gifts, Inducements and Rewards

Vendors are advised to refrain from offering gifts and rewards in any form or manner to any SATS employee in relation to the obtaining or execution of any contract with SATS, whether or not the like acts are performed by the Vendors or persons acting on his/their behalf with or without the knowledge of the Vendors.

SATS shall terminate the Contract, forfeit the deposits and debar the Vendors for any appropriate period of time if it is proven that the Vendors has offered and/or given gifts and rewards in obtaining or in execution of any contract.

3.5.12 Date Compliance

The Services and/or Hardware and/or Software are and will be free from date compliance problems and the performance or the functionality of the Services or obligations to be performed under the Tender and Contract shall not be affected, impeded or interrupted by the entry or processing of any data value or date dependant function, whether such date is past, current or future.

3.5.13 Contract

The successful vendor is required to enter into a Contract with SATS and/or its subsidiaries within fourteen (14) days from the award of the Contract, failing which SATS and/or its subsidiaries reserves the right to award the Contract to another vendor.

3.5.14 Security Deposit

The successful vendor shall pay a deposit equivalent to five (5%) of the annual value of the Contract as Security Deposit.

If the security deposit is below $2,000, the amount shall be paid by a crossed cheque drawn in favour of SATS Ltd, SATS Airport Services Pte Ltd or SATS Catering Pte Ltd or Singapore Food Industries Pte Ltd or any of its subsidiaries, as the case maybe.

If the security deposit is $2,000 and above, a banker's guarantee valid for the period of Contract will be acceptable, provided such guarantee undertakes to meet all claims arising during the period of Contract.

This deposit shall be retained for the duration of the Contract and shall, after liquidated damages, if any, have been deducted, be refunded to the successful vendor at the end of the Contract. No Interest shall be paid on the deposit. The template shown in **Annex 7** (Sample Banker's Guarantee) must be complied with.

Note that security deposit is mandatory and vendors are to comply.

3.5.15 Payment Terms/Scheme

Vendors will follow the Payment Terms/Scheme in accordance with the payment milestones stated by SATS under **Annex 16** (Pricing Table).

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.

3.5.16 SATS Supplier Code of Conduct

The Vendor shall at all times duly comply with the terms of the Supplier Code of Conduct as may be updated from time to time and which may be found at https://www.sats.com.sg/Tenders/Notices/SATS-Supplier-Code-of-Conduct.pdf.

SECTION 4: FORMAT OF PROPOSAL

Each proposal should be structured in a clear, straightforward manner and in accordance with the outline of the respective sections herein. Vendors should exercise care to present only realistic, attainable commitments in their proposal.

Non-compliance to meeting any requirements must be specifically stated with reasons by the Vendors.

Part 1: Tender Forms

All Forms stated below must be presented in the format listed herewith and signed by an authorized signatory.

Enclose within:

1. **Annex 3** (Tender Application Form),
2. **Annex 4** (IPT Declaration by Vendor/Contracting Party)

If the Vendor is a corporation, the **Annex 3** (Tender Application Form) must be signed by an authorized officer of the corporation and stamped with the name of the corporation. No alteration in the **Annex 3** (Tender Application Form) is allowed.

For **Annex 4** (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 2: 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 3: Proposed Solution

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

Proposal could include:

- Functional Hierarchy Diagram (FHD)
- Product overview or technical specifications (including scalability – tpmC, specInt etc., availability – MTBF, MTTF etc.)
- Detailed description of each component or module
- Screen shots of key components or module
- Table of major data fields
- Architecture (functional and technical) diagrams and description
- Security implementation, if necessary
- Solution on interfacing with existing/new systems as defined in the Scope of Work
- Hardware configuration and sizing to meet performance requirements
- Product upgrade path (e.g. details on new functionality/features/architecture and expected date)
- Project management process/methodology, deliverables (e.g. project status etc.) and schedule
- Project organization structure and profile of key project team members (e.g. Management oversight, Project manager, Project leader, Web Creative Designer, Architect, Systems analyst, Main developers, Tester, System administrator, Database analyst, Quality assurance etc), including development team composition i.e. either on-site, off-shore and hybrid model
- 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, development/testing tools to be used, training, transfer of knowledge/skill, secondment of SATS and/or its subsidiaries staff to project team etc.
- Value added services

State:

- the required configuration of your proposed product,
- whether customization of your product is required, keeping in mind that customization must be kept to a minimum and,
- whether integration with SATS's other systems is required and if so, how this is proposed.
- 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.

Software warranty will be for 12 or 24 months' period, commencing from the date of system operational launch.

The Service Level Agreement provided within this RFP must be complied with during the Warranty Period.

Specify the notification period for commencement of any future development work.

Part 4: Prior Experience

Vendors must provide extensive details of a minimum of **03** projects, which they have relevant experience in. These must be similar to the nature of this Tender.

Part 5: Compliance Table

Provide a complete point-by-point response in ALL sections (i.e. Section 3 to **Annex 17** (Standard Contract)). Include any additional information you deemed necessary to support your proposal, explaining how the proposed system would handle each requirement.

Section 3	Tender Procedures
Annex 3	Tender Application Form
Annex 4	IPT Declaration by Vendor/Contracting Party
Annex 5	Individual Non-Disclosure Agreement
Annex 6	Terms and Conditions on Usage of SATS IT Resources
Annex 7	Sample Banker's Guarantee
Annex 8	WSH Rules and Regulations
Annex 9.1	Service Level Agreement
Annex 9.2	Service Level Agreement - Incident Management
Annex 10	Information Security Requirements
Annex 11	Infrastructure and Architecture Standards
Annex 12	IT Operations Standards and Guidelines
Annex 13	IT Coding Practices
Annex 14	Application Maintenance Services
Annex 15	Scope of Work (Detailed)
Annex 16	Pricing Table
Annex 17	Standard Contract ("Contract")
Appendix A (2)	Envelope Label for Tender Submission

This complete point-by-point response shall be done in a form of a Compliance Table as shown in Figure 2 below:

Para. No.	SATS Requirements	Compliance	Remarks
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.

Figure 2: Sample of Compliance Table for Section 3 to Annex 17

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 17** (Standard Contract), in the table format shown in figure 2.

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.

Part 6: Pricing/ Payment Terms

For work covered in this RFP, Vendors must submit a fixed fee proposal (provide price breakdown where possible) within the **Annex 16** (Pricing Table).

The submission of **Annex 16** (Pricing Table) is to be separated from tender proposals, i.e. **Annex 16** (Pricing Table) are not to be filed or bind together with the tender proposal and it shall be filed or bind as a different document. Refer to section 3.3 for instruction of tender submission.

Software licenses and maintenance must be fixed for five (5) years and subsequent annual increase pegged to the CPI in Singapore subject to a maximum increase of one percent (1%), whichever is lower.

Vendors may be required to maintain and support the application/product for an initial contract term one (1) year with an option to extend it each year for the next two (2) years, after which there will be a handover to the SATS or its appointed vendors. Please quote up to a timeframe of five (5) years (individually).

Provide a standard man-day and man-month rate to be used in the commercial proposal for all future application development work. This standard man-day and man-month rate will be effective for the duration of the Contract. Any assessment of Change Requests effort must be made free-of-charge to SATS and/or its subsidiaries.

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

Provide a validity period of nine (9) months from the deadline for Submission of Proposal.

Vendors shall bear any withholding tax, if applicable.

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

ANNEX 3: TENDER APPLICATION FORM

TENDER NO: CT2010J020

DESCRIPTION:

TENDER CLOSING DATE & TIME:

28 December 2020, 1200 Noon Singapore Time

TENDER VALIDITY:

UNTIL NINE (9) MONTHS FROM TENDER CLOSING DATE

TENDER AMOUNT:

Upon submission of tender, the Tenderer shall be deemed to have accepted unconditionally and without qualification all the terms and conditions in the Tender Documents.

Secretary, Tenders Committee
(Non-Foodstuff & Other Equipment)

TENDERER'S FULL BUSINESS/CORPORATE NAME AND ADDRESS

*TENDERER'S GOODS AND SERVICES TAX REGISTRATION NO:

** Please state "NA" if not applicable.*

TENDERER'S CONTACT PERSON'S NAME, TELEPHONE NO, FAX NO AND EMAIL ADDRESS

To: the Company

Words and expressions used in this Form of Tender (which expression when used herein shall include all schedules hereto) shall bear the meanings set out in the Conditions of Tender.

Having examined and fully understood the Tender Documents including without limitation the Conditions of Tender and the Agreement, and assessed all matters and things as may be relevant hereto, we, the Tenderer, hereby irrevocably make an offer to the Company to provide the goods and/or services to the Company as comprised in the Project and more particularly described in the contract specifications, on the terms and conditions set out in the Tender Documents including without limitation the Agreement and the contract specifications, at the pricing and terms as set out in this Form of Tender.

We confirm that we have not relied on any representation or warranty from or made on behalf of the Company in submitting this tender, other than as expressly stated in the Tender Documents.

We confirm that the pricing set out in this Form of Tender is firm and not subject to any adjustment or fluctuation during the contract term.

We agree and undertake that our offer herein shall remain irrevocable and open, valid and binding upon us from the date of submission of this our tender until nine (9) months after the Tender Closing Date, and that the Company may by written notice to us accept our offer herein at any time before the expiration of such period.

Tenderer's business/company stamp

Signature of Tenderer or its authorised signatory

Full Name and Designation of Tenderer's authorised signatory

Date

Nb. No changes are permitted to be made to the terms contained in this Form of Tender.

ANNEX 4: IPT DECLARATION BY VENDOR/CONTRACTING PARTY

DECLARATION BY TENDERER / CONTRACTING PARTY

TO: ....
(Name of SATS Group Company / SATS Entity At Risk)

I/WE, ..., hereby declare that:
(Name of Tenderer / Contract Party)

1) * Our Company is not related (as defined in Section 6 of the Companies Act) to Temasek Holdings (Private) Limited (“Temasek”) or any of its subsidiaries.

2) * Our Company is related to Temasek and/or any of its subsidiaries OR Temasek and any of its subsidiaries has/have an interest in the shares of our Company *(please complete (a) and (d) below)*:

(a) The percentage of the shares of our company in which Temasek and/or any of its subsidiaries has an interest, direct or indirect, is ....% (in total).

(b) Our immediate holding company and ultimate holding company are .... (holding......% of the shareholding of our Company) and ....(having an interest, direct or indirect< in ....% (in total) of the shareholding of our Company), respectively.

(c) Our company is *listed/unlisted.
(If listed, please annex to this Declaration a statement setting out (i) the securities exchange on which your Company’s shares are listed, and (ii) the names of the Directors and Audit Committee members of your Company).

(d) *our Company is a member of a group of companies with listed member(s).
(Please annex to this Declaration a statement setting out (i) the names of the listed member(s) of the group, (ii) how it/they is/are related to your Company, (iii) the securities exchange on which it/they is/are listed, and (iv) the names of its/their respective Directors and Audit Committee members.)

3) I am/We Are *not a Director or Chief Executive Officer or member of the immediate family *(i.e. spouse, child, adopted child, step-child, sibling or parent)* of a Director or Chief Executive Officer, of SATS Ltd. (“**SATS**”).

4) I am/We are *not trustee(s) of any trust of which Director or Chief Executive Officer of SATS, or his immediate family, is a beneficiary or *(in the case of a discretionary trust)* is a discretionary object.

5) I am/We are *not a company in which a Director or Chief Executive Officer of SATS, or his immediate family, has an interest of 30% or more.

I/We confirm that the above information is true and correct. I/We understand that you required the information to comply with Chapter 9 of the SGX-ST Listing Manual.

Date: ....

Signature: ....

Name of Authorised Signatory: ....

Designation of Authorised Signatory: ....

Name of Person/Firm/Company: ....

Company Stamp: ....

Note [*]: Delete as appropriate.

Words and expressions used herein bear the meaning set out in the SGX-ST Listing Manual. Please contact Company Secretary SATS if you require any clarification of this Declaration or any words and expressions used herein.

ANNEX 5: INDIVIDUAL NON-DISCLOSURE AGREEMENT

1.1 Recognition of SATS Services' Rights

At all times during my employment with ____________________________<Name of Vendor> and thereafter, I will hold in strictest confidence and will not disclose, use, lecture upon or publish any of the SATS' Proprietary Information (defined below), except as such disclosure, use or publication may be required in connection with my work for the SATS, or unless an officer of SATS expressly authorizes such in writing. I will obtain SATS' written approval before publishing or submitting for publication any material (written, verbal, or otherwise) that relates to my work at SATS and/or incorporates any Proprietary Information. I hereby assign to SATS any rights I may have or acquire in such Proprietary Information and recognize that all Proprietary Information shall be the sole property of SATS and its assigns.

1.2 Proprietary Information

The term "Proprietary Information" shall mean any and all confidential and/or proprietary knowledge, data or information of SATS regardless of form, format or media, including, without limitation, written or oral information, information in electronic form, whether or not marked "confidential" or the like or expressed to be disclosed as confidential information. By way of illustration but not limitation, "Proprietary Information" includes

(a) trade secrets, inventions, mask works, ideas, processes, formulas, source and object codes, data, programs, other works of authorship, know-how, improvements, discoveries, developments, designs and techniques (hereinafter collectively referred to as "Inventions");
(b) information regarding plans for research, development, new products, marketing and selling, business plans, budgets and unpublished financial statements, licenses, prices and costs, suppliers and customers;
(c) information regarding the skills and compensation of other employees of SATS; and
(d) Personal data belonging to SATS as defined in the Personal Data Protection Act 2012 (Act 26 of 2012) and information and details relating to its directors, officers, and employees.

Notwithstanding the foregoing, it is understood that, at all such times, I am free to use information which is generally known in the trade or industry, which is not gained as result of a breach of this Agreement, and my own, skill, knowledge, know-how and experience to whatever extent and in whichever way I wish.

1.3 Third Party Information

I understand, in addition, that SATS has received and in the future will receive from third parties confidential or proprietary information ("Third Party Information") subject to a duty on SATS' part to maintain the confidentiality of such information and to use it only for certain limited purposes. During the term of my employment with ______________________________ <Name of Vendor> and thereafter, or when I leave my employer, I will hold Third Party Information in strictest confidence and will not disclose to anyone (other than SATS personnel who need to know such information in connection with their work) or use, except in connection with my work for SATS, Third Party Information unless expressly authorized by an officer of SATS in writing.

1.4 No Improper use of Information of Prior Employers and Others

During my employment, I will not improperly use or disclose any confidential information or trade secrets, if any, of any former employer or any other person to whom I have an obligation of confidentiality, and I will not bring onto the premises of SATS any unpublished documents or any property belonging to any former employer or any other person to whom I have an obligation of confidentiality unless consented to in writing by that former employer or person. I will use in the performance of my duties only information which is generally known and used by persons with training and experience comparable to my own, which is common knowledge in the industry or otherwise legally in the public domain, or which is otherwise provided or developed by SATS.

I hereby sign this Non Disclosure Agreement as an addendum to the Agreement signed between ____________________________<Name of Vendor> and SATS with regards to ________________________________ <Name of Project>.

IN WITNESS WHEREOF, the following parties hereto have executed this Non-Disclosure Agreement as of the date stated below.

Team Member	**Project Manager**
--	--
Name:	Name:
Designation:	Designation:
Date:	Date:

ANNEX 6: 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 Entity]** its subsidiaries and associated companies (the " SATS Group") and the SATS Group's networks, systems and assets.

Pursuant to the Agreement dated [ ](“Agreement”) between [Insert Name of Vendor] and SATS, this letter is to confirm your said engagement by SATS will be subject to the terms and conditions of the Agreement, and the following terms and conditions as set out within this Annexure (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. endeavor 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 authorized 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.

h. shall comply with all applicable legislation, rules and regulations relating to the protection of privacy and personal data in the transmission and storage of data.

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 organization;

   iv. circulating "chain letters" or spreading rumors;

   v. distributing third party copyright materials;

   vi. distributing trade secrets or sensitive corporate information which may cause damage to the organization, 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 unauthorized 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 authorization 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 authorization 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 unauthorized 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 endeavor 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.

[For employers only] I undertake to pay a penalty of a minimum 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:

Name:
Designation:
Company:
Date:

ANNEX 7: SAMPLE BANKER'S GUARANTEE

[insert date]

SATS Ltd.
SATS Inflight Catering Centre 1
20 Airport Boulevard
Singapore 819659

Dear Sir/Madam,

OUR BANK GUARANTEE NO.*[INSERT NUMBER]* FOR SINGAPORE DOLLARS *[INSERT AMOUNT IN WORDS]* ONLY (S$*[INSERT AMOUNT IN NUMBERS]*)

In consideration of yourselves, SATS Ltd. of SATS Inflight Catering Centre 1, 20 Airport Boulevard Singapore 819659 ("SATS") having agreed to enter into an agreement for the supply and delivery of *[insert item]* (the "**Agreement**") with ***[insert name of Contractor]*** of *[insert address of Contractor]* (the "**Contractor**") under which SATS agreed to allow the Contractor to furnish the security deposit payable under the Agreement by way of a banker's guarantee, we, ***[insert name of Bank]*** of *[insert address of Bank]* (the "**Bank**") hereby unconditionally and irrevocably guarantee and undertake to make payment to you of up to the maximum aggregate sum of **Singapore Dollars *[insert amount of the security deposit in words]* Only (S$*[insert amount of the security deposit in numbers]*)** (the "**Guaranteed Sum**").

The Guaranteed Sum, or such part or parts thereof as may be specified by you in your written demand to the Bank made from time to time, shall be payable by the Bank in full immediately upon first written demand by you, without any set-off, counterclaim or deduction whatsoever.

The Bank shall not impose any condition or qualification for/in making any payment to SATS pursuant to such demand, nor shall the Bank make any reference to the Contractor prior to making such payment. The Bank shall make such payment demanded notwithstanding any notice or demand from the Contractor not to do so.

The Bank shall not at any time be concerned as to whether there is any breach by SATS or the Contractor or any dispute between SATS and the Contractor in respect of any terms and conditions of the Agreement. This Guarantee and the Bank's liability under this Guarantee shall not be determined, discharged or released or in any way affected, prejudiced or impaired, by:-
(a) any indulgence, forbearance or concession given by SATS to the Contractor (whether as to payment, time, performance or otherwise);
(b) any arrangement made with the Contractor or any other person;
(c) any variation of the terms and conditions of the Agreement;
(d) any lack of capacity or authority on the Contractor's part in executing the Agreement; or
(e) any insolvency, winding up, liquidation, bankruptcy or dissolution of the Contractor,

whether known to or agreed by the Bank or otherwise.

The Bank's obligations under this Guarantee are that of a primary obligor and not merely as surety, and the Bank hereby waives all rights which it might otherwise as surety be entitled to claim and enforce.

This Guarantee shall be irrevocable and shall remain in full force and effect at all times throughout the period from **the date of this Guarantee up to and including *[insert date falling 2 months after the date of expiry of the term of the Agreement]*** (both dates inclusive) (the "**claim period**"). Notwithstanding this, we hereby undertake to extend the validity of this Guarantee as and when requested by you in writing at any time before the expiry of the claim period. Demand may be made under the Guarantee by SATS at any time and from time to time during the claim period. Upon expiry of the claim period, all liability of the Bank shall cease under this Guarantee, notwithstanding that this Guarantee is not returned to the Bank for cancellation.

This Guarantee shall be governed by and construed in all respects in accordance with the laws of the Republic of Singapore and the Bank hereby submits to the non-exclusive jurisdiction of the Singapore courts.

____
[insert name of signatory]
[insert title of signatory]
for and on behalf of
[insert name of Bank]

ANNEX 8: WSH RULES AND REGULATIONS

All vendors (including but not limited to) subcontractors, agents etc. must conform fully with the Ministry of Manpower's requirements in the Risk Management Regulation readily available on their website.

1.0 General

1.1 Ensure their workers and sub-contractors have the required qualifications, competencies or licenses to carry out specific activities that may be required by Singapore's Laws & Regulations.

1.2 Ensure all instruments, machineries; tools (including hand-tools, electrical and mechanical tools) or vehicles must have the appropriate certificates, permits or licenses from the relevant authorities before it may be used inside SATS premise.

1.3 Ensure all machineries, tools or vehicles are properly and safely used as per their purpose and design. No modification shall be made unless otherwise approved by the manufacturer or relevant authorities.

1.4 Use of SATS tools, equipment or machineries is not allowed without the prior approval of the SATS Work Coordinator.

1.5 All operating permits, licenses or apparatus granted by the relevant local authority are to be submitted to the WSH Personnel on demand or upon request prior to any work commencement.

1.6 Observe and adhere to all posted "Danger", "Warning", "Caution" and "Notice" signs.

1.7 Smoking is strictly prohibited within SATS premises except at Designated Smoking Area.

1.8 Lockout and Tag out should be implemented when servicing, inspecting, repairing, cleaning or maintaining machineries or equipment in SATS where the unexpected energization, start-up or release of stored energy sources could cause injury to the worker.

1.9 Risk Assessment MUST be conducted and established for works as prescribed in the WSH Risk Management Regulation.

1.10 Comply with all applicable Singapore Workplace Safety and Health legislations, regulations & others requirements, inclusive of SATS safety rules and regulations.

2.0 Hazard Areas

2.1 Certain areas/rooms and operation within SATS site where, because of the nature of the hazards, extra precautions must be taken. Before entering any of the following areas or starting work on any operation within these areas, the contractor is required to check with the SATS Work Coordinator for a review of applicable WSH rules:

2.1.1 High Voltage Electrical Areas
2.1.2 Waste Water Treatment Plant
2.1.3 Chemical Storage Areas
2.1.4 Utility Shafts housing, Overhead Pipes and Ducts and Confined Spaces

3.0 Overhead Work

3.1 No overhead work shall commence if any person is present or over roadways or passageways until adequate precautions have been taken to ensure the safety of persons and property below.

3.2 Relocation of personnel shall be accomplished prior to and maintained throughout the overhead work period. The contractor shall make all personnel relocation requests to the SATS Work Coordinator.

3.3 Contractors are not permitted to crawl along and/or step on ductworks, cable trays, pipings or other building structures.

4.0 Housekeeping

4.1 Materials should be carefully stacked and located so that it does not block Aisles, Doors, Fire Fighting Equipment, Eyewash Stations, First Aid Boxes, SDS Stations, Chemical Spill Kit, Fixed Ladders, Electrical Equipment or Stairways.

4.2 Nails protruding from board must be removed.

4.3 Concrete form and scrap lumber and all other debris shall be kept clear of all work areas.

4.4 Combustible scrap, waste materials and debris shall be removed from the building on a daily basis, preferably at the time of strip-out and disposed of at the designated collection points.

4.5 Overhead storage of debris, tools, equipment, pipes, etc. is prohibited. No loose material shall be left in the area above suspended ceiling panels.

4.6 The work area shall be kept free from any potential tripping hazards.

4.7 Do not obstruct passageways and exits.

5.0 Floor Openings

5.1 Substantial barriers, railings, and covering material shall guard floor openings. The contractor shall supply all materials required to cover the floor openings.

6.0 Chemicals

6.1 Contractors must submit the most recent copies of the Safety Data Sheets (SDS) to the SATS Work Coordinator for any chemicals they plan to use in SATS premises. All SDS must be submitted and approved for use by WSH Personnel prior to the contractor starting work.

6.2 All chemicals used shall be in their original container with the original vendor labels or proper-labeled secondary container. The labels must include chemical constituents, hazard information, safety precautions and proper use specifications.

6.3 Contractors are responsible for conducting "Hazard Communication" sessions for their workers and Sub-Contractors in accordance with governmental requirements.

6.4 All work with chemicals shall be carried out with minimal exposure to contractor and SATS personnel.

6.5 All chemicals for the contract shall be purchased and supplied by the contractor, unless the contract specifically states otherwise. The proper disposal of used chemicals is at the expense of the contractor.

6.6 The Contractor is advised that there are some areas of SATS where hazardous chemicals are present. It is the contractor's responsibility to review all areas of his work and determine if a hazard to his personnel exists. Upon request, SATS will provide the necessary information for the contractor regarding hazardous chemicals used in our facilities.

6.7 Prevent contaminated water from escaping into open drains and/or public sewer. Prevent any spill causing water and soil contamination.

6.8 Contractors shall not store any chemicals at SATS premises, including overnight storage, unless prior approval by the SATS Work Coordinator.

6.9 Adequate ventilation must be provided and maintained at all times when flammable and/or toxic chemicals are used.

6.10 Flammable, oxidizer and corrosive liquids must never be stored together.

7.0 Ladders

7.1 The contractor is required to provide his or her own ladders, with company identification clearly visible. In no case shall contractors utilize SATS ladders for carrying out their work.

7.2 When using a ladder in aisles, lobby, cafeteria or any other area that has free access to personnel and is not designated as a "construction area", the area around the ladder is to be barricaded with ropes and stanchions, cones or another contractor employee to direct personnel around the ladder work area.

7.3 The use of ladders with broken or missing steps/rungs, broken side rails or with other faulty or defective construction is prohibited.

7.4 Ladders shall not be placed adjacent to a door unless the door is locked or guarded.

7.5 Metal ladders shall not be used when working on any electrical systems unless properly insulated.

7.6 The contractor shall not use any ladders in an unsafe manner. This includes, but is not limited to, standing on the top step as well as No 2nd party holding the ladder.

7.7 Ladders are not to be set-up and left unattended. Ladders not in use should be stored in a secure area.

7.8 Permit-To-Work at Height would be required for any work above 2m.

8.0 Compressed Gas Cylinders

8.1 Any compressed gas cylinder taken into the SATS must be in good condition, correctly labelled and content identified.

8.2 Compressed gas cylinders shall be secured (roped or chained) in an upright position at all times. Use of forklift as a mean of transportation is prohibited unless a special structure is used to uphold the cylinders.

8.3 Cylinders shall be kept a safe distance or shielded from welding and cutting operations. Cylinders shall not be placed where they can contact an electrical outlet or outdoor exposed to the sun and rain.

8.4 Cylinder valve protection caps shall be firmly installed (hand tight) when compressed gas cylinders (empty or full) are transported or stored.

8.5 The correct regulators, in proper working order shall be used for each type of gas. Regulators or regulator connections shall not be modified in any way.

8.6 Dual Fashback arrestors must be provided on each welding hose.

9.0 Tools

9.1 Contractor shall provide their own hand and power tools required for the work. Tools shall not be provided or loaned out by SATS.

9.2 Tools used must be of safe construction and maintained.

9.3 When working near or inside flammable storage areas, spark resistant tools should be used to prevent the hazard of friction spark that may be an ignition source.

9.4 Defective tools must not be used. It shall be tagged and removed from the work site immediately.

10.0 Scaffolds

10.1 Suitable and sufficient scaffolds should be provided for workers for all work that cannot be safety done at height from a ladder or by other means.

10.2 All types of scaffolds must be erected, used and supervised by contractor in accordance with governmental requirement.

10.3 Permit-To-Work at Height is required when contractor erects fixed or mobile scaffolds in SATS.

11.0 Cranes And Hoists

11.1 Contractors shall not be permitted to use SATS hoists without prior permission from SATS Work Coordinator.

11.2 Crane lifts shall not be attempted over or adjacent to any occupied areas. If such work is necessary, it shall be coordinated with the SATS Work Coordinator and the occupied area shall be evacuated of all personnel prior to the lift.

11.3 Hoisting devices such as slings, chains, spreaders, grabs, etc., used in conjunction with hoists or cranes must be designed and fabricated to meet the Work requirements. Swivel type, self-catching safety hooks shall be used for the load hook.

11.4 Contractors' cranes and hoists used at SATS must meet governmental and other regulatory requirements and have current certifications available for examination as required.

12.0 Electrical

12.1 The contractor shall not perform any work on **ENERGIZED** (Live) electrical panels, distribution boards, bus ways or other electrical devices, which may expose personnel to accidental contact with energized parts.

12.2 All electrical equipment should be equipped with electric grounding unless they are manufactured as a double insulated equipment.

12.3 Extension cords shall be the three-wire type for grounded tools (two-wire is acceptable for double insulated tools) and shall be protected from damage. Worn or frayed cords shall not be used. Cords must not be run through doorways where the door could cut or damage the cord. Spliced cords must be connected with proper connector and not insulation tape.

12.4 No wiring shall be left on the floor ground or the floor where there is vehicular or human traffic. If unavoidable, the wiring must be provided with adequate mechanical protection to withstand the wear and abuse to which it may be subjected.

12.5 Portable electrical tools should be equipped with a Residual Current Device for earth leakage protection.

12.6 Do not overload any electrical circuit.

13.0 Excavation

13.1 All excavation works must be carried out in accordance with governmental and other regulatory requirements. The detection of underground utilities should be conducted prior to the excavation.

13.2 Inform WSH personnel before the start of any excavation work.

14.0 Personnel Protective Equipment

14.1 The type of protective equipment to be worn shall be determined by the degree of exposure to potential hazards. All protective equipment and clothing shall be provided by the contractor and shall comply with all applicable regulations and requirements.

14.2 Suitable eye protection equipment shall be used while engaged in welding, cutting or grinding any material where flying particles may endanger the eyes.

14.3 Safety harness must be worn when working above 2 meters on unguarded platforms and on straight or extension ladders when the work involves pushing, pulling or action, which may dislodge the person from the ladder. DO NOT SECURE SAFETY HARNESS TO THE SPRINKLER OR UTILITY PIPINGS.

14.4 Hard Hat and safety shoes must be worn at the designated areas. Hearing Protection must be worn when using noisy equipment that generate noise of more than 85dBA or working in areas which are identified as high noise level. Areas with high noise level are identified with "Ear Protectors Must Be Worn" Notice Sign.

15.0 Accidents And First Aid

15.1 Contractors who are injured shall be given prompt and proper medical attention at the SATS Inhouse Clinic or first aid station by certified first aiders.

15.2 Contractor must notify their Work Coordinator immediately in case of any accident/incident or first aid cases.

15.3 Assist Work Coordinator to furnish the Incident & Near-Miss Investigation Reports.

15.4 It is the contractors' responsibility to notify relevant authorities as required under prevailing laws.

16.0 Confined Space Entry

16.1 Confined Space Entry Permit is required when contractors are carrying out work in confined space. Confined spaces are areas that may have atmospheric or physical hazards that could affect the safety of employees who enter them. It is not designed for continuous human occupancy and has a limited means of entry or exit. These areas include, but are not limited to pits, tanks, duct, manholes and trenches.

16.2 The Contractors are responsible for the full compliance of the conditions attached within the approved Confined Space Entry Permit.

17.0 Hot Work

17.1 Hot Work Permit is required when contractors perform Hot Work, i.e. work that involves welding, flame cutting, gas soldering, brazing, burning or any work that generate sparks.

17.2 The Contractors are responsible for the full compliance of the conditions attached within the approved Permit.

18.0 Emergency Response & Action

18.1 Familiar with the escape routes and assembly area in case of any emergency. Check with the SATS's Work Coordinator for a review of applicable *Emergency Evacuation Instructions*.

18.2 Main Contractor's Supervisor is responsible for accounting their own employees & Sub-Contractors working in SATS in the event an emergency wh er e evacuation is required. He/she shall inform SATS's Work Coordinator if any person is not accounted for.

18.3 Know the nearest location of the emergency response equipment such as eye wash station, first aid station and fire extinguishers etc.

~ **The foregoing WSH RULES AND REGULATIONS stated in the above paragraphs shall continue to be enforced for all your subsequent work engagement with SATS.**

~ **The Main Contractor shall be responsible for briefing these rules and regulations to any Sub-Contractors or any person contracted or employed by them.**

~ The Main Contractor shall be responsible for the actions of its Sub-Contractors while inside SATS premises.

==

I hereby sign this WSH Rules and Regulations as an addendum to the contract agreement signed between **[INSERT NAME OF VENDOR]** and **SATS** with regards to **[INSERT PROJECT NAME]**.

IN WITNESS WHEREOF, the following parties hereto have executed this WSH Rules and Regulations as of the date stated below.

For and on behalf of **[INSERT NAME OF COMPANY]**	Witness By:
---	---
Signature & Company Stamp	Signature & Company Stamp
Name Designation Date:	Name: Designation: Date:

ANNEX 9.1: SERVICE LEVEL AGREEMENT FOR WARRANTY PERIOD AND APPLICATION MAINTENANCE SERVICES (AFTER WARRANTY PERIOD)

1. MAINTENANCE SUPPORT & HELPDESK HOURS

All Vendors shall quote for two options for maintenance support and helpdesk to all users:

a. Option A: Daily (8.00am – 8.00pm)
b. Option B: 24 X 7 days

2. INCIDENT MANAGEMENT

Vendors will need to comply with SATS's incident management flow (refer to **Annex 9.2** (Service Level Agreement - Incident Management)).

3. PROBLEM RESOLUTION CRITERIA

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

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

4. SERVICE LEVEL FOR WARRANTY PERIOD AND APPLICATION MAINTENANCE SERVICES (AFTER WARRANTY PERIOD)

4.1 SEVERITY LEVEL, RESPONSE TIME AND RESOLUTION TIME

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	2 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

4.2 DEFINITIONS OF SEVERITY LEVELS

Severity Level	**Description**
1	An Incident or Problem shall be assigned as “Severity Level-1” if: • The Incident or Problem causes or will potentially cause Major Business Impact, which affects a Widespread User Base.
2	An Incident or Problem shall be assigned as “Severity Level-2” if: • The Incident or Problem causes or will potentially cause Major Business Impact, which affects a localized user base; and/or • The Incident or Problem is not affecting the normal operation or use by Authorized Users of any Critical Systems, but affects a Widespread User Base.
3	An Incident or Problem shall be assigned as “Severity Level-3” if: • The Incident or Problem causes or will potentially cause Minor Business Impact; and • There is no Acceptable Workaround for the Incident.
4	An Incident or Problem shall be assigned as “Severity Level-4” if: • The Incident or Problem causes or will potentially cause Minor Business Impact; and • There is an Acceptable Workaround for the Incident.

4.3 DEFINITIONS AND INTERPRETATION

Term	**Definition**
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, 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.

4.4 SERVICE CREDITS FOR NON-COMPLIANCE OF SERVICE LEVELS DURING WARRANTY PERIOD AND APPLICATION MAINTENANCE SERVICES (AMS) (AFTER WARRANTY PERIOD)

In the event of a Service Level default (where the Vendor is unable to meet the Service Level stipulated in Section 4.1 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, ie. If Service Level default occurred in Jan 2014, the SCUs are to be paid in Feb 2014. 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	NA
Severity level 3	NA
Severity level 4	1

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

Value per SCU = Sum x At Risk Amount x Allocation factor / 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 1 (as per table above) x no. of months (twelve (12) months during AMS)

The Vendor acknowledges and agrees that the Service 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.

4.5 SERVICE CREDITS FOR NON-COMPLIANCE OF SERVICE AVAILABILITY AND TRANSACTION RESPONSE TIME SERVICE LEVEL

Service credits for non-compliance of Service/System Availability and Transaction Response Time targets will be as follows:

Category	Service Levels	Service Credits for Non-Compliance of Service Levels
Service/System Availability	[Target Service/System Availability to be filled in. (example: 99%)]*	[Example: Actual Downtime – Planned Downtime Allowed * (15% of Monthly Transaction Fee) Subject to maximum amount]*
Transaction Response Time	98% of the transactions below 2 seconds	2% of Monthly Transaction Fee for every 3% of monthly Transactions that fail the Target Transaction Response Time. Subject to maximum amount

The Vendor acknowledges and agrees that the Service 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.

4.5.1 DEFINITIONS OF NON-COMPLIANCE

Term	Explanation
Service/System Availability	Total time minus both Scheduled Outages and Unscheduled Outages in that month, expressed as a percentage of the total time of that month. **% Measured System Availability** = $\frac{\textbf{Total Time – Scheduled Outages – Unscheduled Outages)}}{\text{(Total Time – Scheduled Outages)}} \times 100$
Actual Downtime	Total time of service unavailability (includes Planned and Unplanned downtime)
Planned Downtime Allowed	A planned downtime is the time agreed by both parties for maintenance activities with prior notice.
Unplanned Downtime	An unplanned period of time, when the service is not accessible at the time the service is scheduled to be accessible in accordance with the provisions of the Agreement.
Transaction Response Time	ASP: Time taken from the moment an input message from SATS reaches the Service provider server until the output is delivered from the Service provider server. Blackbox/Whitebox: Time taken from the moment an input message reaches the Application until the output is delivered from the Application.

ANNEX 9.2: SERVICE LEVEL AGREEMENT – INCIDENT MANAGEMENT

1. INCIDENT MANAGEMENT

Vendors will need to comply with SATS's incident management flow.

2. SMITH PROCESSES

2.1. Resolver Acceptance*

Roles and Responsibilities

1. Allocate initial resource to assess the Incident
2. Assess the Incident details and Check whether the ticket is correctly referred;

- If the Incident has been **incorrectly** referred:-
  (i) Update the ticket with the following :-
    a) information as to what problem determination steps were performed
    b) who the ticket should be referred to (if known)
  (ii) For high severity Problem Tickets (Severity 1 & 2), follow up with a phone call to SMITH Call Centre/Command Centre (depending on the originator of the call)
  (iii) Transfer the ticket back to SMITH Call Centre/Command Centre (depending on the originator of the call)

- If the Incident has been **correctly** referred :-
  (i) Assess the assigned Incident Severity;
  (ii) If it is deemed that the Incident Severity is incorrect then contact SATS by phone to discuss directly with the User. Based on the outcome of the conversation with SATS do the following:-
    a) If the customer agrees to your preferred Severity:-
      1. Contact the SMITH Call Centre by phone.
      2. Inform them that the customer has agreed to change the severity.
      3. Ask the SMITH Call Centre to update the ticket with the new severity.
    b) If the User does not agree to a change in the severity:-
      1. Update the ticket with the details of the conversation including the user's reasons
      2. Report to your line management and continue to work on the Incident at the assigned severity.
  (iii) The Resolver should accept the Incident by updating the ticket in the system
  (iv) Prioritize the Incident by severity

Please note: -

1. For high severity Problem Tickets (Severity 1 & 2), there may be insufficient time for Reassignment of Problem Tickets, therefore the owning Resolver Group must **only** attempt to reassign high severity Problem Tickets where there is sufficient time left for the new Resolver Group to respond & resolve within the SLA period.
2. The owning Resolver Group must co-ordinate with other Resolver Groups as required to analyze and resolve the problem
3. If the Resolver Group of high severity problems requires assistance from other Resolver Groups, they may ask Command Centre to co-ordinate etc
4. For high severity Problem Tickets (Severity 1 & 2), the Resolver must work closely with Command Centre and SMITH Call Centre to provide the latest updates of the problem incident. Command Centre will keep the SATS ITS Management informed. SMITH Call centre will keep the users informed.
5. For high severity Problem Tickets (Severity 1 & 2), Command Centre/SMITH Call Centre will monitor the situation closely and perform the necessary escalation when there is a potential breach/actual breach of SLA.

* For Vendors providing for offsite (ie. their staffs are not stationed in SATS's premises), SATS or the appointed vendor will appoint a coordinator who will liaise with the Vendor to access and update the incident ticket.

2.2. Incident Resolution

Roles and Responsibilities

1. Assess facts and fact finding of the incident. Check with the User if the details in the ticket is insufficient.
2. If the Incident is deemed to be a Security Breach or a significant* Virus event, inform SATS ITS Management immediately
3. Ascertain whether there is a workaround
4. If so, Raise Request for Change according to SATS Change Request Process. Apply the workaround, update ticket with workaround details and update the status of ticket to 'Resolved'.
5. If no workaround available:-
   a. Ascertain whether more resources are required.
      If required, then assign additional resources or work with line manager for the resources required.
   b. Update ticket with time taken to resolve problem.
   c. Commence work to resolve problem
   d. Upon completion of work, update ticket with details of resolution and amend status of ticket to 'Resolved'

2.3. Incident Closure

Roles and Responsibilities

1. Contacts the User to discuss any outstanding issues regarding the incident.
2. Resolves incident and updates the incident ticket will the details of incident resolution.
3. Updates incident ticket with resolution details if ticket is transferred back by SMITH due to lack of resolution information or after confirmation with the User that the incident has not been resolved.

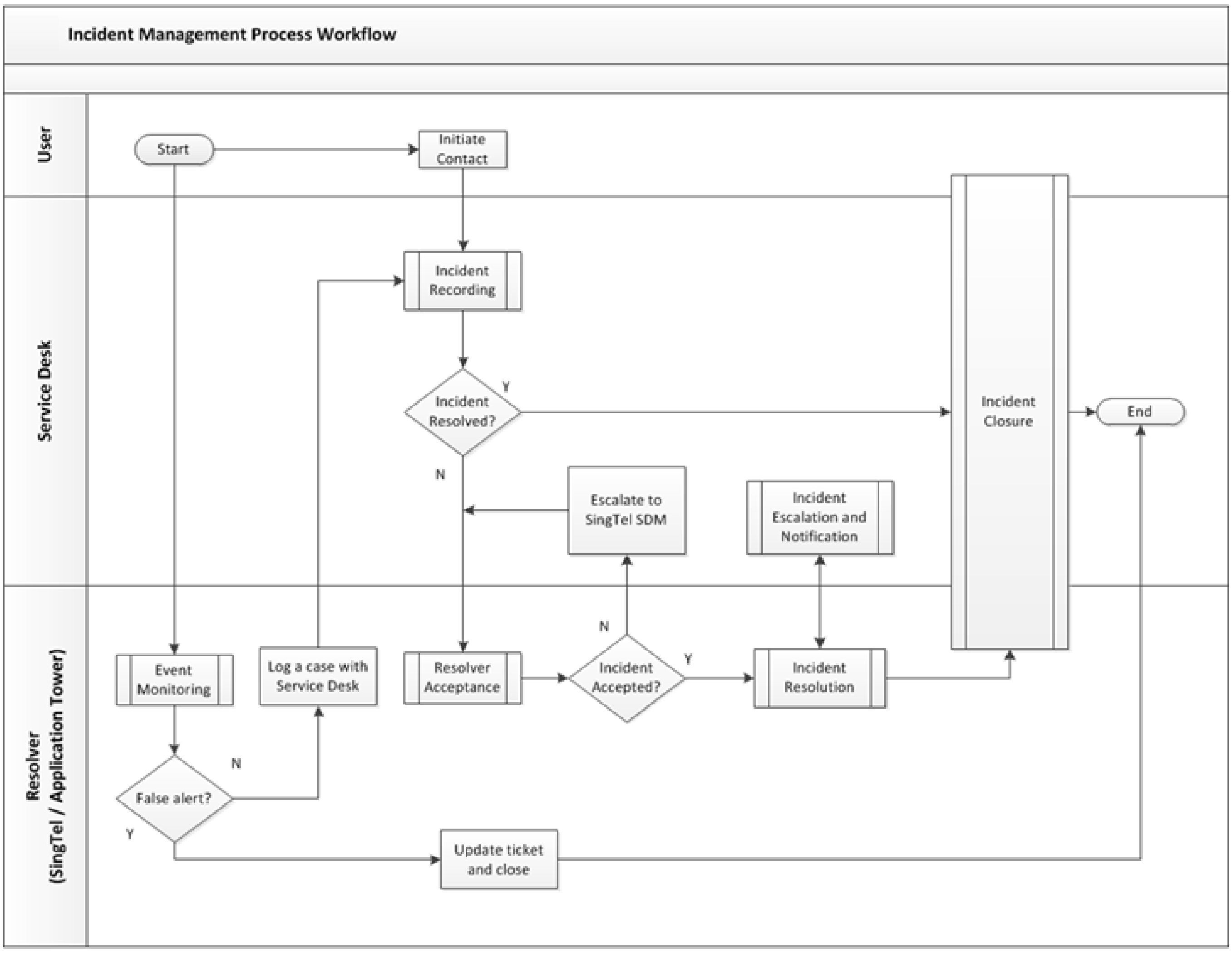
If the User requests for the closure of the incident, and the Resolver is already working on the Incident and wishes to continue, then update incident ticket accordingly. Add note with comments that the User had requested the Incident be closed however the Resolver is still working on the Incident. This will be logged as a Bug Fix activity with the appointed Vendor.

Note: Resolution details should be acceptable in order to go with incident closure. List down the steps/actions taken to solve

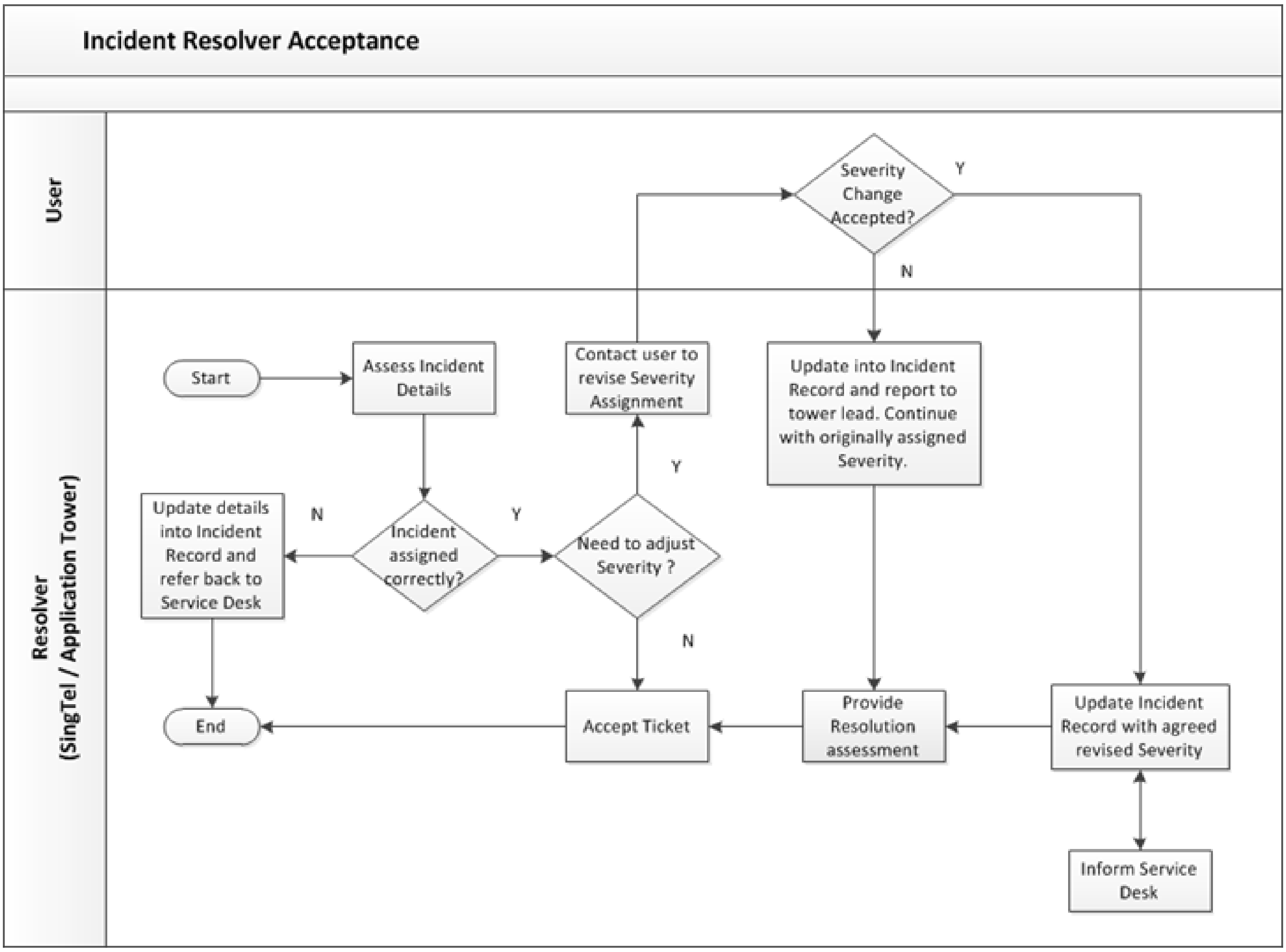
4. SMITH is the only entity that can close an Incident ticket with the agreement of the User. A closure request can be from:

   - User who may have an intermittent problem or the problem has "gone away";
   - Resolver who has resolved the Incident;
   - SMITH Call Centre who resolves it at first call resolution.

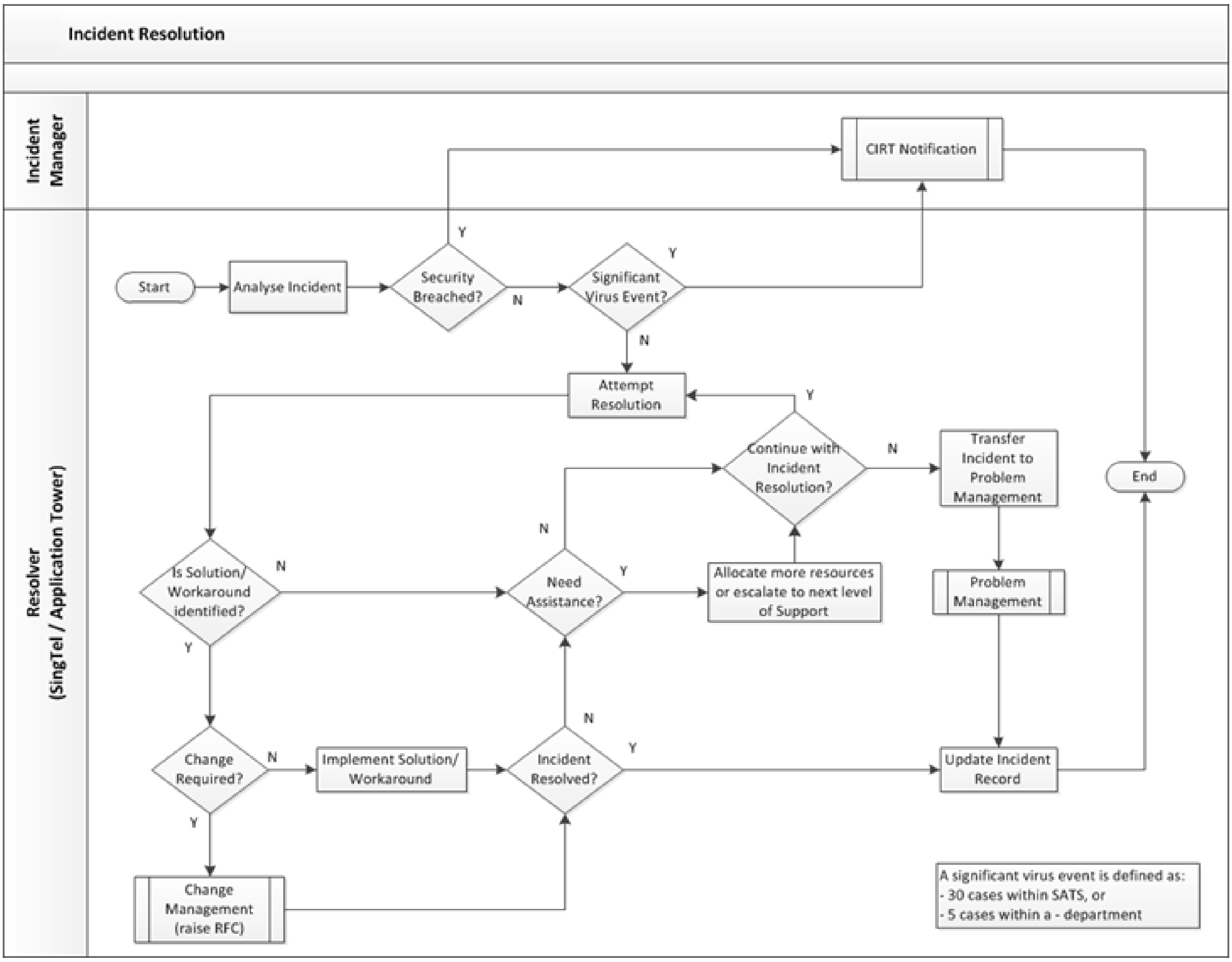
INCIDENT MANAGEMENT PROCESS OVERVIEW



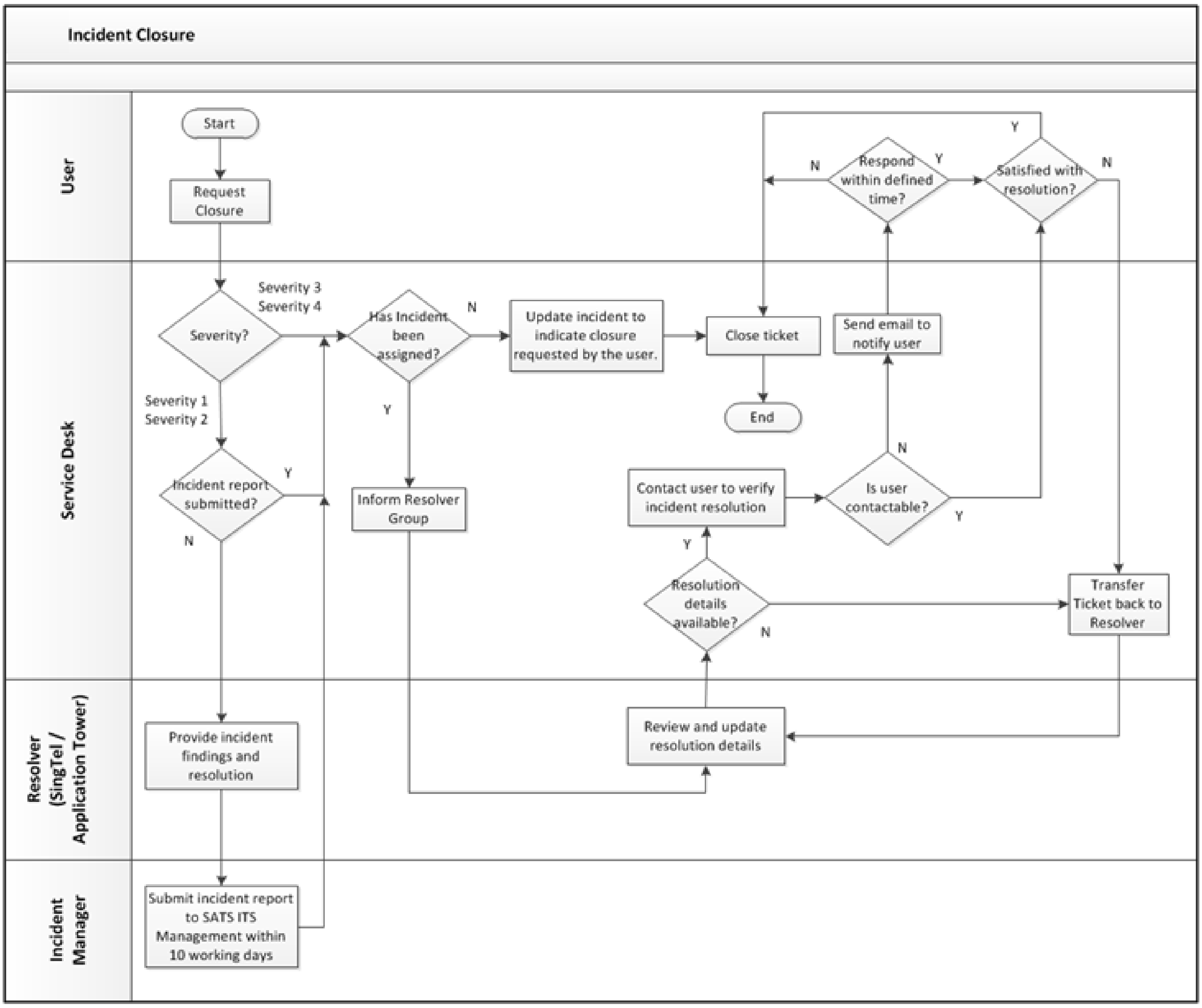
RESOLVER ACCEPTANCE PROCESS


Incident Resolver Acceptance
User
Resolver (SingTel / Application Tower)
Severity Change Accepted?
Y
N
Start
Assess Incident Details
Contact user to revise Severity Assignment
Update into Incident Record and report to tower lead. Continue with originally assigned Severity.
Y
Update details into Incident Record and refer back to Service Desk
N
Incident assigned correctly?
Y
Need to adjust Severity ?
N
End
Accept Ticket
Provide Resolution assessment
Update Incident Record with agreed revised Severity
Inform Service Desk

INCIDENT RESOLUTION PROCESS


Incident Resolution
Incident Manager
Resolver (SingTel / Application Tower)
CIRT Notification
Start
Analyse Incident
Security Breached?
Y
N
Significant Virus Event?
Y
N
Attempt Resolution
Y
Continue with Incident Resolution?
N
Transfer Incident to Problem Management
End
N
Is Solution/ Workaround identified?
N
Y
Need Assistance?
Y
Allocate more resources or escalate to next level of Support
Problem Management
N
Change Required?
N
Y
Implement Solution/ Workaround
Incident Resolved?
Y
Update Incident Record
Change Management (raise RFC)
A significant virus event is defined as:
- 30 cases within SATS, or
- 5 cases within a - department

INCIDENT CLOSURE PROCESS


Incident Closure
User
Service Desk
Resolver (SingTel / Application Tower)
Incident Manager
Start
Request Closure
Severity?
Severity 3 Severity 4
Severity 1 Severity 2
Has Incident been assigned?
N
Y
Update incident to indicate closure requested by the user.
Close ticket
End
Send email to notify user
Respond within defined time?
N
Y
Satisfied with resolution?
Y
N
Incident report submitted?
Y
N
Inform Resolver Group
Contact user to verify incident resolution
Is user contactable?
N
Y
Resolution details available?
Y
N
Transfer Ticket back to Resolver
Provide incident findings and resolution
Review and update resolution details
Submit incident report to SATS ITS Management within 10 working days

ANNEX 10: 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, its subsidiaries and associated companies (the "SATS Group") and the SATS Group's networks, systems and assets.

General

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 and protection of SATS resources from its other customers.

1.7 Software that, intentionally or otherwise, has known vulnerabilities, attempts or has any possibility to exploit the security of SATS' systems shall not be used.

Logs Management

1.8 System logs shall be centrally stored and secured for possible forensic use. These would include but not limited to servers, routers, databases, intrusion detection system, firewall, and application audit trail and access logs.

1.9 Audit logs shall include sufficient information to establish what events have occurred, who or what has caused them, and when did the events happened.

1.10 Establish procedures and processes for the monitoring and review of audit logs and the prompt reporting of security-related alerts on violations such as intrusion detection, unauthorised access or modifications.

1.11 Procedures and processes shall be documented, reviewed and updated regularly with SATS.

1.12 The retention period of logs and audit trails must comply with legal and regulatory requirements.

Security Incident Handling

1.13 Immediately report any security incident involving their systems, and/or SATS IT resources to SATS, and cooperate with the investigation as required.

1.14 Ensure availability of services is maintained and take responsibility for the security incident.

1.15 Provide logs in its native format without any alteration when requested.

1.16 Provide an Investigation Report detailing the cause of the security incident, action done, and remediation/mitigation plan.

Disaster Recovery (where applicable)

1.17 Ensure availability of hot-site facilities.

1.18 Annual performance of recovery tests.

1.19 Ensure back-up procedures are established and functional.

Protection of assets

1.20 Implement procedures and/or solutions to protect SATS assets, including information, hardware and software.

1.21 Implement procedures and/or solutions to determine whether any compromise of the assets has occurred.

1.22 Implement controls to ensure the return or destruction of information and assets at end of, or at an agreed point in time, during the contract.

1.23 Implement controls on restrictions of copying and disclosing of SATS information.

1.24 Implements processes and solutions to ensure protection against malicious attacks.

1.25 Personal computing devices not issued by SATS shall not be connected to SATS' network before explicit approval has been granted by SATS IT Services. Such approvals shall be temporary with a stated end date.

1.26 Upon approval, users of personal computing devices not issued by SATS must ensure that these devices are free from malicious codes and are equipped with endpoint firewall and anti-virus software with up-to-date virus definition files before connecting to SATS' resources.

Access Control

1.27 Ensure access to SATS' business information is restricted to authorized personnel supporting SATS' systems

1.28 Implement physical and logical access controls to restrict and limit access to authorized areas and granted based on valid business requirements only.

1.29 Third parties shall not be allowed to access SATS' resources and network through the Vendor's network.

1.30 Use of network sniffing tools is prohibited unless authorized by SATS.

1.31 Only use access methods approved by SATS, with appropriate controls and use of unique identifiers such as User IDs.

1.32 Establish an authorization process to authenticate all access, including users and administrators, to SATS resources.

1.33 Maintenance of an authorized user list and what their rights and privileges are with respect to each account.

1.34 Access by the Vendor's personnel/subcontractors/agents to SATS resources must be reviewed periodically to ensure currency of those personnel/subcontractors/agents and their access rights.

1.35 The Vendor must immediately notify SATS and remove from access when an account is no longer required.

1.36 Accounts must not be shared. All users requiring access to SATS resources must have unique user IDs and owned individually.

1.37 All privileged access and activities must be logged and the log files and audit trails must be protected to facilitate future audit and investigations.

Regulatory Compliance

1.38 Subject to the Cybersecurity Act 2018, Personal Data Protection Act (PDPA) and/or any relevant data, patent, copyright and privacy protection legislation within Singapore or where SATS resources are hosted.

1.39 Subject to any intellectual property rights and copyright assignment and protection of collaborative work within Singapore or where SATS resources are hosted.

Non-disclosure of information

1.40 Discovery of security vulnerabilities on SATS resources shall not be disclosed, and shall be reported to SATS immediately.

1.41 Details of SATS network, applications or other information that the Vendor may have access to during the course of contract with SATS shall not be disclosed to any third parties, directly or indirectly.

Change Management

1.42 Changes to production systems must be documented, reviewed and authorized and implemented in a controlled manner in accordance with established procedures to prevent accidental and unauthorized modification and destruction. All relevant documentation pertaining to the changes implemented should be updated to reflect the changes.

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

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

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

Application Security [*for application system – remove if not applicable*]

1.46 Application development environment must be segregated from the production environment.

1.47 Conduct application secure code reviews where possible throughout the system development phase for quality assurance.

1.48 Perform Vulnerability Assessment and Penetration Test before deployment to production or deployment of any major change[1].

1.49 Provide reports to SATS detailing the findings of Vulnerability Assessment and Penetration Test, including the vulnerability identified and targeted remediation date.

1.50 All vulnerabilities identified from vulnerability assessment and penetration tests must be remediated within the following duration:

Severity	To Be Remediated
Critical/High	4 weeks from issuance of Report
Medium and Low	8 weeks from issuance of Report

1.51 Vulnerabilities identified from Vulnerability Assessment and Penetration Test must be remediated and approved by SATS before production launch or deployment of major change.

1.52 Manage and replace SSL/TLS certificate(s) before its expiry with the contract period.

Mobile Management [*for mobile application development – remove if not applicable*]

[1] Major change refers to when a new major function/module is introduced, or when there is an addition or change to system codes and the effort required is more than 15 man days.

1.53 Ensure mobile application is compatible to SATS Mobile Device Management (MDM) solution prior to deployment;

1.54 Cost of effort, if required, to secure connectivity and communication between mobile application and server through SATS MDM shall be borne by Vendor unless agreed and approved by 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 Audit 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 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.

2.7 Undertake the required validation procedures according to the agreed Service Provider Level, and provide SATS the equivalent reports that they are required to submit to the payment brands or acquiring banks based on their Service Provider Level.

2.8 Indemnify SATS for any security breach resulting in loss of information, misuse of personal data, or credit card information due to Vendor's non-compliance of PCI DSS.

ANNEX 11: INFRASTRUCTURE AND ARCHITECTURE STANDARDS

1. SATS Desktop/Notebook Client Environment

1.1. The vendor shall ensure that the system is able to run on the following desktop/notebook environment setup used in SATS:

- Microsoft Windows 7 SP1, Microsoft Windows 10 Enterprise and above
- Internet Explorer 11 and above
- Java Runtime Environment 1.8 and above
- Anti-virus and personal firewall
- No local administrator rights
- Client software distribution using MSI format run in silent mode

1.2. If the system needs to run on a minimal set of specifications for the desktops/notebooks used in SATS in terms of processor, clock speed, CPU cores and memory, the vendor needs to provide such details in their proposal.

2. Server Environment

2.1. If the solution is to be deployed on an On-Premises setup within SATS Data Centre, the following environment setup should be conformed:

- Operating System
  - Windows Server 2016 or later
  - Red Hat Enterprise Linux 7.5 and above
  - Solaris 11.4 or later
- Web server
  - IIS 10.0 and above
  - Apache HTTP Server 2.4 or later
- Application Server
  - IIS 10.0 and above
  - Oracle WebLogic 12c R2 or later
- Relational Database
  - Oracle 12c R2 or later
  - MS SQL Server 2016 or later
- Network and Security Services
  - File and Print Server: Windows 2008
  - Site-to-site VPN for data exchange and production/UAT/development environment support
  - Single sign-on using Active Directory Federation Services (ADFS) or a SAML 2.0 compatible Identity and Access Management platform
- Data Centre (DC) Operation
  - IT Service Management and System Management/Monitoring using DC-provided tools
  - Backup, File System Management and HA/Clustering using DC-provided tools
  - Application Onboarding managed by SATS On-Premises Managed Services Vendor
  - OS Patching managed by SATS On-Premises Managed Services Vendor

2.2. If the solution is to be deployed on Cloud-based infrastructure hosting, the environment shall conform to the infrastructure and architecture standards of the respective Cloud Provider. SATS is currently using Microsoft Azure Cloud to host its Cloud-based applications.

3. Middleware / Application Services

3.1. Asynchronous Services:

a. All new asynchronous services must be built on the JMS open standards.

b. All new asynchronous services must support the publish & subscribe model and dedicated point-to-point queue model.

3.2. File Transfer Services:

a. If the system requires to perform file transfer, all file transfers shall go through SSH File Transfer Protocol (SFTP) mode only.

b. If the system generates an output file from a batch job meant for file transfer purposes, the output file should be sent to a centrally managed file server for distribution to third-party or downstream consuming applications. The system should either push the output file to the centrally managed file server or the centrally managed file server should pull the output file over.

c. If the system requires to retrieve an input file provided by third-party or another application, the input file should be obtained from a centrally managed file server. The system should either pull the input file from the centrally managed file server or the centrally managed file server should push the input file over.

3.3. Batch Jobs / Batch Processing:

a. If the system requires to run batch jobs to perform batch processing, the system shall automatically manage all batch input and output files without operator intervention. Operator must not be manually putting in the batch input file, or transferring the batch output file to another location.

b. All batch jobs shall be triggered without any need for operator intervention. Any job dependencies must also be handled by the system without any operator intervention.

c. All batch jobs should be capable to perform auto-recovery without operator intervention.

d. The system shall have a capability to track when each batch job was triggered, when each batch job ends, and whether the batch job was successful or had failed. If the batch job fails, there must be logs written by the system that provides the details of the failure.

3.4. Authentication Services:

a. For a system requiring authentication functionality and the user base is SATS users, the system should integrate with SATS' Active Directory service and ADFS (Active Directory Federation Services) to perform Single Sign-On (SSO) access between applications.

b. The system shall be designed to support the following methods for integration with ADFS:
- SAML 2.0
- OAuth 2.0

c. The system should be designed to support integration with a future centralised Identity and Access Management (IAM) platform that provides:
- Centralised authentication and password reset
- Centralised access rights management (at role/group level)
- Single-Sign-On (SSO) between systems that are integrated with IAM

d. The system shall be designed to support the following methods for integration with the future central IAM:
- SAML 2.0
- OAuth 2.0

3.5. Application Programming Interfaces (APIs):

a. The system should be designed to expose re-usable functionalities via RESTful API calls.

b. All re-usable API functions designed for the system shall be exposed and published through the centralised API Gateway provisioned by SATS.

c. All APIs developed for publishing to the API Gateway shall conform minimally to the following best practices:

1) Nouns should be used, not verbs
2) Use plural nouns, instead of singular nouns
3) Versioning must be present (e.g. v1, v2)
4) Use hyphens in URIs rather than underscores if there is a need to have multiple words in the URI (e.g. overseas-customers)
5) CRUD (i.e. Create, Read, Update, Delete) should not be used in the API URI to indicate actions performed. Use the HTTP request methods to indicate actions performed instead

4. Architecture Design / Setup

4.1. The system shall be designed using a 3-tier architecture (i.e. Web tier, Application tier, Data tier).

4.2. The system shall be designed to run on Virtual Machines (VMs). Usage of hardware appliance or physical servers should be avoided unless there is a technical limitation.

4.3. The system shall have a separate User Acceptance Test (UAT) environment from the Production environment.

4.4. The system shall have a similar architecture setup for both Production and UAT environments. Examples of non-similar setup are:
a. 2-tier architecture setup in UAT but 3-tier in Production
b. Load Balancer is configured for Production but not configured for UAT
c. 2 Database instances used in Production but 1 shared Database instance used in UAT

4.5. The system shall use a user-friendly URL to resolve and access the website (e.g. https://lms.sats.com.sg). Server hostnames and port numbers must not be exposed at the URL (e.g. https://satswebserver1:8080/lms).

4.6. The system's website(s) shall not use port numbers other than 80/443 unless required technically and with appropriate justification.

4.7. The system shall use the latest version of software or software packages. The system is allowed to use an earlier release version of software or software packages if there are compatibility issues. The earlier version shall be 1 major release earlier than the latest version (e.g. if the latest version of SQL Server is 2017, the earlier version allowed is SQL Server 2016, if the latest version of a software is ver 8.x, the earlier version allowed is ver 7.x, unless there is a version number jump in between versions).

4.8. The system shall have a backup and recovery process tested, validated and documented prior to system rollout.

4.9. The system shall define a clear criteria for performance testing, and all performance benchmarks should be met prior to system rollout.

4.10. The system shall implement automatic log files rotation.

4.11. The system shall define a housekeeping/archival policy for transactional data (e.g. audit trail records) and application log files.

4.12. The vendor shall define a proper incident management and escalation flow that combines Level 1 incident reporting using SATS' Incident Management vendor (SMITH) with the provider's Level 2 and Level 3 support. Handover documentation shall be provided to SMITH prior to SMITH taking over the Level 1 support.

4.13. If the system is implementing a custom-developed mobile app for corporate or internal users' usage, the mobile app shall be compatible with SATS' Mobile Device Management (MDM) platform, Samsung EMM.

5. Application Security

5.1. The system should have the following security services enforced:
a. Process in place to review user access rights on a periodic basis
b. Audit Trail and Events Logging
c. Security Hardening (on Operating System and Middleware)
d. Security Code Reviews been performed
e. Vulnerability Assessment conducted / to be conducted
f. Penetration Test performed / to be performed by an authorised third party vendor
g. Distributed Denial-of-Service (DDOS) Protection
h. Anti-Defacement Services
i. Intrusion Detection / Prevention System (IDS/IPS)
j. Web Application Firewall (WAF)

5.2. The system shall be security-hardened at the middleware layer, for those middleware software provided or installed by the vendor. Examples of some middleware software that are to be hardened by the vendor: Apache HTTP Web Server, Apache Tomcat, SharePoint.

5.3. Security hardening of the system shall take relevant guidelines / benchmarks from the Center for Internet Security (CIS) at https://www.cisecurity.org/.

5.4. If the system is an internet-accessible application, a SSL SHA256 (or above) certificate from a Certificate Authority (CA) shall be used and installed on either a Load Balancer or Web Server(s) to encrypt all client-to-server traffic.

5.5. If the system needs to store user passwords in the database, a secured hash algorithm shall be used for the encryption of the passwords (e.g. bcrypt, SHA-512), so that the passwords are not in clear-text.

5.6. If the system needs to store passwords in a configuration file (e.g. application/database account password), a secured symmetric encryption method (i.e. encryption and decryption using the same key) shall be used for the encryption of the passwords, so that the passwords are not in clear-text.

5.7. If the system needs to store personal data like PDPA-related data, the data should reside in Singapore (e.g. hosted in a database where the infrastructure is located in Singapore).

6. Software Support

The Vendor's responsibilities shall include:

(i) Unless otherwise directed by SATS, ensuring that the Software is supported at the version (the "N" release level) stated within.

(ii) As directed by SATS, also ensuring that the Software is supported by the release N-1 and earlier versions of the Software for the longer of:
(a) The thirty-six (36) month period following version N's general public availability.
(b) The time the Software vendor ceases to support such version.

(iii) Using commercially reasonable efforts to maintain the Software that is no longer supported by the Software vendor.

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

7. Software-as-a-Service (SaaS) Standards

7.1. If the solution is a SaaS, the SaaS vendor shall provide certified report(s) that certify that their software have complied with strict security, quality and audit controls and have met international and industry-specific compliance standards (e.g. ISO9001:2015, ISO27001:2013, 3rd party security test audit certificates, etc).

7.2. The SaaS provider should provide relevant incident response plan to SATS for review.

7.3. The SaaS provider should provide past reports of vulnerability assessment and penetration test performed to SATS for review.

7.4. The SaaS provider should ensure that there are no risks/vulnerabilities exposed at the time of delivery.

ANNEX 12: IT OPERATIONS STANDARDS AND GUIDELINES

All vendors must adhere to the Standards and Guidelines that has been provided within this Annex. Should there be any deviations, Vendors must state clearly in the proposal and all costs associated with the deviations.

There are 3 areas in which all Vendors must take note of:
(a) Code Deployment
(b) Batch Processing
(c) Monitoring Agent

1. Compliance Criteria

- Functional IDs should be provided for different functional groups (e.g. IT Operations, Application Maintenance etc).

- Deployment Testing is mandatory to ensure that the application is available after code deployment. This is conducted after every code deployment (e.g. upgrades, patches etc). Vendors must provide means of allowing this testing to be done.

2. Deployment Pack (must be provided by Vendors):

- Roll forward and Roll Back scripts must;- (a) be provided in an "executable" mode and (b) be suffixed with the application name & server name (eg. Rollforward_XXX_68.sh/rollback_XXX_68.sh for application XXX and the server is capsxp68).

- Roll Forward scripts must;- (a) have a prompt as to whether to continue or abort when executing the script, (b) have a backup of files for recovery use, (c) take care of deleting & adding of application without having to log in to a console and (d) extract new/updated files into their respective folders.

- Roll Back scripts must;- (a) have a prompt as to whether continue or abort when executing the script and (b) be capable of restoring the changes to its original state.

3. Batch Processing

If Batch Processing is required, Vendors must ensure:

- Management of all batch input/output (data transfer)
- Batch jobs must be processed without operator intervention
  - Job dependencies must be handled within or across systems
- Job Scheduling must be automated
- Job Return
  - Batch job must be capable of auto-recovery without operator intervention

4. Monitoring Agent

- All critical application processes must be monitored by monitoring tools provisioned by SATS Managed Services vendor.

ANNEX 13: SATS CODING PRACTICES

All vendors must adhere to the SATS' standard coding practices that have been provided within this Annex. Should there be any deviations, Vendors must state clearly in the proposal and all costs associated with the deviations.

Please take note that SATS will not be liable to incur any additional costs which is not stated in Vendors' proposal.

1. **Input Validation**

1.1. A centralized input validation routine (against allowed characters and entries).
1.2. Validate all client provided data before processing, including all parameters.
1.3. Validate data from redirects (which might just circumvent application logic and any validation performed before the redirect).
1.4. Validate for expected data types.
1.5. Validate data range.
1.6. Validate data length.
1.7. Validate all input against a list of allowed characters, whenever possible.
1.8. All validation failures should result in input rejections.
1.9. If any potentially hazardous characters must be allowed as input, vendor(s) must be responsible to implement additional controls, secure task specific APIs and account for the utilization of the data throughout the application.

2. **Data Protection**

2.1. Implement least privilege; users access should be restricted to only the functionality, data and system information that are required to perform their task.
2.2. The application should support the removal of sensitive data when that data is no longer required.
2.3. Do not store passwords, connection strings or other sensitive information in clear test or in any non-cryptographically secure manner on the client side.
2.4. Encrypt highly sensitive stored information, including but not limited to, authentication verification data, even on the server side. Using well vetted algorithms should be applied at all times.
2.5. Protect all cached or temporary copies of sensitive data stored on the server from unauthorized access and purge those temporary working files as soon as they are no longer required.
2.6. Implement appropriate access controls for sensitive data stored on the server. This includes but not limited to, cached data, temporary files and data that should be accessible only by specific system users.

3. **Database Security**

3.1. Utilize input validation and meta characters must be addressed. If these fail, do not run the database command.

// A **metacharacter** is a character in a program or data field that has a special meaning (instead of a literal meaning) to a computer program. Examples of meta characters includes * ; |] [? //

3.2. The application should use the lowest possible level of privilege when accessing the database.
3.3. Close the connection as soon as possible.
3.4. The application should be connected to the database with different credentials for every trust distinctions (e.g. user, read-only users, guest, and administrator).
3.5. Removal of permissions should be allowed to the base tables in the database.
3.6. Connection strings should not be hardcoded within the application. Connection strings should be stored in a separate configuration file on a trusted system and should be encrypted.

4. **Memory Management**

4.1. Double check that the buffer is as large as specified.
4.2. When using functions that accept a number of bytes to copy, such as strncpy(), be aware that if the destination buffer size is equal to the source buffer size, it may not NULL-terminate the string.
4.3. Whenever there is a calling of the function in a loop, check buffer boundaries and make sure there is no danger of writing past the allocated space.
4.4. Specifically close resources and properly free allocated memory upon completion of functions and at all exit points.

5. **File Management**

5.1. Do not save files in the same web context as the application. Files should be either go to the content server or in the database.
5.2. Ensure applications files and resources are read-only.
5.3. Scan user uploaded files for viruses and malware.

6. <u>Error Handling</u>
6.1. Do not disclose sensitive information in error responses, including but not limited to, system details, session identifies or account information.
6.2. Implement generic error messages and use custom error pages.
6.3. The application should be able to handle application errors and not rely on the server configuration.
6.4. Properly free allocated memory when error conditions occur.
6.5. By default, error handling logic associated with security controls should be denied.

7. <u>Logging</u>
7.1. All input entries MUST be logged.
7.2. Ensure logs contain important log even data
   - Time stamp from a trusted system component
   - Severity rating for each event
   - Tagging of security relevant events, if it is mixed with other log entries
   - Identify of the account and/or user that caused the event
   - Source IP address associated with the request
   - Event outcome, either success or failure
   - Description of the event

7.3. Restrict access to logs to only authorized individuals/users.
7.4. Use a master routine for all logging operations.
7.5. Ensure that a mechanism exists to conduct log analysis
7.6. For privilege IDs, all access to the system and database must be logged. This log must be reviewed on a regular basis for “abuse” or illegal activities.

8. <u>General Coding Practices</u>
8.1. Do NOT hardcode
8.2. Use tested and approved managed code rather than creating new unmanaged code for common tasks.
8.3. Utilize task specific built-in APIs to conduct operating system tasks. Do not allow the applications to issue commands directly to the Operating Systems, especially through the use of application initiated command shells.
8.4. Utilize locking to prevent multiple simultaneous requests to use a synchronization mechanism to prevent race conditions.
8.5. Protect shared variables and resources from inappropriate concurrent access.
8.6. Explicitly initialize all your variables and other data stores, either during declaration =or just before the first usage.
8.7. In cases where the application must run with elevated privileges, raise privileges as late as possible, and drop them as soon as possible.
8.8. Review all secondary applications, third party code and libraries to determine business necessity and validate safe functionality, as these can be introduce new vulnerabilities.
8.9. Restrict users from generating new code or altering existing code.
8.10. When conducting unit testing of the developed codes, vendor(s) must test all boundary conditions to ensure that it is being well taken care of in the program.
8.11. All assumptions, including but not limited to, high level logic design, and specific comments to further explain the logic must be explicitly documented in the program itself for ease of troubleshooting and maintenance by others. For the avoidance of doubt, all documentations shall belong to SATS.
8.12. All relevant SATS policies pertaining to Information Security (InfoSec), Personal Data Protection Policy (PDPP), architecture standards, etc. must be adhere to in the program design and coding practices.

ANNEX 14: APPLICATION MAINTENANCE SERVICES

1. Applications Maintenance

Vendors may be required, upon the request of SATS, maintain and support the application/product ("Software") for an initial contract term of one (1) year with an option to extend each year, thereafter. However the final decision will be at SATS' sole discretion. Details and scope of application maintenance and support for the Software includes:

1.1. Solve problems reported including making changes to the following items (includes but not limited): (1) programs, (2) configuration parameters, (3) database, (4) file system and (5) data. This will also include answering of queries from SATS. There should be sufficient information logged for debugging.

1.2. Work with relevant parties with regards to maintenance of hardware, OS, database, server software and other standard system software to resolve problems in their respective areas.

1.3. Troubleshoot Software problems with interfaces to external systems, including validating data coming-in/going-out and implementing any program changes required, etc.

1.4. Investigate system performance problems and implement ways to improve performance

1.5. Manage version controlling of software, configurable parameters and documents.

1.6. * Managing version control includes liaising with SATS and/or other SATS appointed vendors performing changes to the same system(s) if any.

1.7. Maintain up-to-date documentation of systems, applications, interfaces and operation manuals.

1.8. Provide necessary technical support and consultation on queries on Software, to SATS and/or other SATS appointed vendor(s) to carry out enhancements or software upgrades to the system(s), and/or to develop new system(s) and/or to develop interfacing system(s).

1.9. Provision for necessary onsite support activity for major upgrades (Major release).

1.10. Assist SATS' internal/external/security auditors with their queries.

1.11. Maintain a knowledge database of list of problems and solutions for future use by SATS. Note that the Knowledge Database will be owned by SATS.

1.12. Prepare Service Level Agreement (SLA) compliance reports, incident reports, enhancement status reports, production release reports and weekly and monthly status reports as per the preferred format in vendor guide.

1.13. Provide support for Software running on production, testing, disaster recovery and training environment wherever applicable. This includes packaging of Software components for deployment and installation of Software and configuring of parameters if any.

1.14. Provide scripts to make any changes to databases and/or files and coordinate with relevant parties to carry out the changes.

1.15. Manage Software development environment. This includes installation of OS, Database (upgrades & changes), Software, server software, necessary tools and configuring of parameters if any.

1.16. Provide preventive maintenance and continuous improvement to reduce number of failures and improve stability and availability of system.

1.17. Perform necessary Software testing / implement system changes required to migrate applications to run on newer versions of compilers/ tools, OS, server software and/or databases.

1.18. For interfacing systems that are maintained by SATS and/or other SATS appointed vendors, provide necessary support to solve problems in their Software.

1.19. Install Software and relevant tools in client PCs/laptops that are required for the application, working with SATS IT Helpdesk for the installation.

2. Minor Enhancements

2.1. Undertake Software enhancements including testing, documentations, conduct user acceptance test, rollout and support.

2.2. The Vendor must work and coordinate with relevant parties whenever necessary, towards delivery of the enhancement. The relevant parties include the users, infrastructure personnel or infrastructure appointed vendors, and external parties including but not limited to SITA, ARINC and Government bodies for application certification and/or application deployment.

2.3. Guidelines for enhancement requirements are stated below:

Size of enhancements	Vendor to respond with solution proposal & cost estimate
< 1 man month	Within 3 working days
< 3 man months	Within 5 working days
> 3 man months	Within 10 working days

2.4. Provide training to users on any enhancements being implemented if required.

2.5. The Vendor must deliver the enhancement within the timeframe agreed upon with SATS.

3. General Requirements

3.1. * The Vendor is required to support any changes or enhancements done to the system(s), irrespective of whether such changes are implemented by SATS and/or other SATS appointed vendors. Actively participate in ensuring the smooth and complete handover of such changes or enhancements by the other parties.

3.2. Software support should cover applications that are used in Singapore as well as those that are used at overseas stations.

3.3. For offshore and off-site development and support, the Vendor will be required to provide their own hardware and software.

3.4. SATS will provide the necessary hardware and required software for the User Acceptance Test (UAT) and Production environments. In all cases, the Vendor is required to adhere to the Infrastructure and Architecture Standards as shown in Annex 11 (any deviations must be approved by SATS).

3.5. The Vendor is required to adhere to SATS defined processes described in the AMS Vendor Guide and/or Third Party Supported Applications Vendor Guide and/or Application Service Provider (ASP) Supported Applications Vendor Guide for solving problems and carrying out of enhancements. A copy of relevant Vendor Guide whichever is applicable will be provided while awarding the contract.

3.6. The Vendor is required to use SATS's management tools for (includes but not limited to): (1) source code management, (2) problem management, (3) change management and (4) configuration management, as directed by SATS. Do note that no other management tools used and/or proposed by the Vendor will be used, unless otherwise agreed by SATS.

3.7. * Upon expiry or termination of the 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 and on-the-job training to SATS staff and/or SATS appointed vendors. This will be at no additional costs to SATS.

3.8. The Vendor is required to meet the SLA for application maintenance services as shown in **Annex 9.1** Service Level Agreement for Warranty Period, in **Annex 9.2** Service Level Agreement – Incident Management, and in **Annex 14** Application Maintenance Services (After Warranty Period)).

3.9. All enhancements and/or developments will adhere to the existing platforms as stipulated by SATS, unless otherwise stated by SATS.

3.10. All enhancements are to be built on SATS's production release version and that if enhancements can only be built on version higher than SATS's production release version, or project requires a higher release version, project scope must include the product release upgrade and support.

3.11. The Vendor can choose to support some of the work using staff based offshore provided the service levels and other requirements can be met in a cost effective manner. This will be subjected to the approval of SATS.

3.12. The Vendor is required to provide details of the support structure including escalation procedures and processes for incident and change management in the proposal. Any subsequent changes should be communicated to SATS.

3.13. The Vendor is required to adhere to SATS's Information Security Requirements as shown in Annex 10, in all circumstances.

3.14. For offshore and off-site development and support, the Vendor may be given limited and restricted access to SATS network as specified in Annex 10 (subjected to the approval of SATS). Moreover, the Vendor is required to use secured environment for that purpose and provide their network diagram to SATS.

3.15. For Application Service Provider (ASP) solutions, the ASP Vendor is required to:

a) Provide a support hotline/helpdesk for problem reporting

b) Propose a model to track the volume of transactions

c) Provide outage notification at least 10 working days in advance of the planned outage. Unplanned outage should be communicated with outage reason to SATS immediately.

Legend:

* *Applicable only for SATS custom build applications*

ANNEX 15: SCOPE OF WORK - DETAILED

1. REQUIREMENTS SUMMARY

Brief Overview	To develop and deliver an autonomous delivery robot for last-mile runs between raw food preparation area and main kitchen in SFS, 234 Pandan Loop facility.
Business Objectives	The project aims to increase the efficiency and productivity of delivery tasks by automating what was previously a manual effort.
Desired Implementation	End March 2021

2. OBJECTIVE

2.1 SATS is seeking to appoint a vendor ("appointed Vendor") to design, develop, implement (including project manage) and maintain an autonomous delivery robot that can aid in the towing process of pallet jack and trolley loaded with raw food materials from the preparation area to the kitchen.

2.2 The scope of the autonomous delivery robot project includes:

a. Design and development of autonomous delivery robot and its accessory control/operational devices such as emergency stop button, power supply and management devices.

b. Delivery of one (1) Autonomous Guided Vehicle (AGV).

c. Implementation shall be done at SATS Food Services Pte Ltd (SFS), 234 Pandan Loop warehouse and the vendor shall work with SATS to ensure successful implementation.

d. Maintenance and support operations of the AGV.

2.3 The AGV solution must be scalable to cater for follow-on phases which may include enhancements such as integration with a fleet management system as customers demand increases.

2.4 The overall objectives are:

a. Automate the current manual process of towing pallet jacks and trolleys by leveraging on AGV to allow human counterparts to take on more rewarding, value-added work.

b. Ensure a safer and more productive working environment.

2.5 The proposal shall demonstrate ability to design an easy-to-use and responsive system that addresses objectives of SFS.

3. PROJECT SCOPE

3.1. The appointed Vendor shall manage the end-to-end implementation for this project (including but not limited to):

a) Prepare functional specifications, design, develop and deploy the AGV to be used by staff at SFS, Pandan Loop.
b) Setup and installation of all necessary software programs for the AGV will be performed.
c) Trials and testing to be done.
d) Provide training on troubleshooting operations, charging etc to operators and key users.
e) Deliver safety briefing to demonstrate the functions and various safety features of the AGV.
f) Maintenance and support the system after go-live.

3.2 The following highlights the transformation which this project aims to achieve.

(A) Current Process Flow

1. Staffs work from 0200 to 1900, Monday to Sunday.
2. Manual towing of loaded equipment, the maximum payload of 500kg per trip for pallet jack and 200kg per trip for trolley from preparation area to the kitchen.
3. The repetitive, mundane task of moving heavy loaded equipment is laborious and strenuous requiring considerable effort and fatigue to staff.
4. The ability to get new employees into the business and attract people into this type of work is a real challenge especially during peak periods when sales spike.

(B) Future Process Flow

1. With the introduction of AGV, operation will start from 0800 to 1900, Monday to Sunday.
2. The AGV will now pull the loaded trolley and pallet jack with food items and return the equipment back.
3. Provides automation benefits – allowing redeployment of the staff to other value-added tasks, creating less strenuous work conditions, increasing overall output and improving work efficiency leading to enhanced overall productivity without changing current work processes.

4. PROJECT REQUIREMENTS

4.1 The appointed Vendor shall:

a) Implement the project diligently, efficiently and in a timely manner with reasonable care and skill according to the standards in the industry for similar services.

b) Conduct regular meetings with SATS (e.g. SATS Project Steering Committee and Project Team) and Technology PM to update on the progress of the project. Minutes of all meetings conducted must be recorded by the appointed Vendor for future references and final approval of such minutes of meetings shall be sought from the respective Committee Chairperson. Minutes of all meeting shall be submitted 3 working days after meeting date and final approval of the minutes shall be provided 5 working days by SATS after the minutes of meeting submission.

4.2 All Vendors shall adhere to the deliverables list expected for this project provided in **Annex 15**.

4.3 The requirements outlined here shall be used as the baseline requirements. Upon award, the appointed Vendor will conduct detailed design workshops with the various stakeholders to materialize these requirements for the implementation.

4.4 In addition to the agreed requirements, all Vendors are encouraged to propose additional functions, processes and/or procedures which value-add to SATS.

4.5 Operating Environment

4.5.1 The AGV operates in sheltered indoor environment.

4.5.2 It is likely AGV will also encounter an assortment of equipment like motorized forklifts and pallet jacks.

4.5.3 Persons or other equipment may occasionally veer into the path of AGV.

4.6 Vendor shall conduct site survey/s as is necessary to analyse and determine the optimal number of AGV to be deployed at any given time, and the method of deployment. The results of this may be used to justify for subsequent purchase of additional AGV in later phases.

4.7 The Vendor shall collect data of daily AGV operations. These shall include (but not be limited to):

a) Date, time, location of AGV
b) Mileage of individual AGV

5. <u>TECHNICAL REQUIREMENTS</u>

5.1 <u>General Requirements</u>

5.1.1 The AGV shall be able to navigate on its own with minimal setup and preferably no installations to the existing infrastructure.

5.1.2 It is easy to train robot.

5.1.3 It is configurable to tow pallet jack.

5.1.4 It is configurable to pull 2x food trolleys.

5.1.5 To be able to compensate for stability and propulsion even when towing maximum combined load of 600kg.

5.1.6 All electronic components and enclosures shall be designed for IP54 rating as a minimum.

5.1.7 Vendor shall produce relevant documents as proof that all components and systems of the unit are capable of withstanding the conditions stated above, during submission of proposal.

5.1.8 AGV shall have a maximum operating speed of 4kph when fully loaded. Speed between 0 and 4kph should be variable so that acceleration is gradual.

5.1.9 AGV shall be operable in all intended modes on 1:10 slopes (6°) with the maximum carrying load regardless of upward or downward inclines. Brakes applied whilst on slope shall hold the AGV without backward/forward slippage. This function is applicable whilst in both individual and convoy travel modes.

5.1.10 Should be able to carry a load of up to 600kg while operating in its intended environment.

5.1.11 Shall be sufficiently stable for safe operation even if carrying or towing maximum load and travelling on standard accessible slopes.

5.1.12 Where applicable, the System shall comply to SATS existing Cybersecurity Policies and Standards.

5.2 <u>Safety and Security Requirements</u>

5.2.1 AGV design shall comply with internationally recognised health, safety and environment standards (e.g. CE certified).

5.2.2 AGV shall comply with internationally recognised standards for safe operation in areas with high human traffic. The vendor shall include in proposal any standards that are referenced.

5.2.3 AGV shall be equipped with sensors that allow it to detect and avoid any obstacles in its path.

5.2.4 A minimum of one (1) STOP device shall be installed within easy reach of nearby person.

5.2.5 AGV shall stop safely when faced with a detected unsurmountable obstacle, or when STOP button is pressed. When this happens, it shall signal to nearby staff by both visual and audio means that assistance is required. This signaling shall continue until help is rendered.

5.2.6 There should be a means to indicate visually when an AGV is in operation and when there is an error.

5.2.7 AGV brake shall be applied when it is powered down to prevent unauthorised use or runaway. The brakes shall be fail-safe and only released when a user authorises its (AGV) use.

5.2.8 The AGV shall be put in a safe state whenever it is being charged or left unattended for a long time. By safe state, it means the brakes are applied and none of the external controls will cause movement of AGV.

5.2.9 There shall not be edges or surfaces with sharp or pointed features which can potentially cause injuries to pedestrians nearby.

5.3 Electrical Power Requirements

5.3.1 AGV shall be electrically powered and suitably earthed for safe operation.

5.3.2 Each AGV shall be able to operate continuously for at least 11 hours per day with opportunistic charging.

5.3.3 A full charge cycle shall not last more than 6 continuous hours.

5.3.4 Charger shall be compatible with Singapore standard three pin socket (230V and 50Hz).

5.3.5 Charging can be done by plugging direct to a wall socket or by removing a depleted battery and replacing with a full charged battery. Both options shall be made available.

5.3.6 Battery should be easily and safely removed/replaced. Removable batteries shall have an accompanying charger that plugs into a standard 3-pin wall socket.

5.3.7 Battery chargers should have built-in management system to prevent overcharging and prolong the life of the batteries.

6 USER TRAINING

6.1 All Vendors shall propose, conduct and implement a training plan to ensure that all SATS users are competent in order to perform the necessary AGV operation prior to and after implementation of system. This includes the tasks, style of delivery, recommended class size, duration, deliverables and training materials needed for the training plan.

6.2 The System shall be designed intuitively and not require extensive training.

7 TESTING & ACCEPTANCE

7.1 The appointed Vendor shall:

a) Work with all relevant 3rd party vendors (if any) for the integration testing to ensure the installed hardware/software is able to support the requirements stated;

b) Produce the Test Plan documents including Testing Strategy, Test Scenarios and Test Scripts for all phases of testing. These documents shall be subject to SATS' amendments and final approval;

c) Conduct unit functional testing, system integration testing and user acceptance testing;

d) Ensure that all components / systems are tested for successful installation; and

e) Make accurate records of all tests and shall furnish ALL test certificates and schedules of the test results in an approved form mutually agreed by both parties. One (1) original copy of such records and each test certificate shall be submitted to SATS for review.

7.2 All tests shall be conducted in the presence of appointed representative/s from SATS to the satisfaction of SATS.

7.3 Vendors shall supply all necessary testing software tools. Connections and skilled labour required for the tests to be carried out to the satisfaction of SATS, without separate charges to SATS.

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

7.5 Unit Functional Testing (UFT)

7.5.1 The vendor shall conduct its own functional tests on each AGV prior to delivery to SATS. These tests should aim to ensure the AGV can perform all its stated functions as per the requirements. SATS representatives shall be allowed to attend and witness these tests.

7.5.2 A check-list showing all parameters tested shall be jointly created and submitted as proof of successful testing.

7.5.3 Everyday maintenance and functional issues like battery charging shall be demonstrated.

7.6 System Integration Testing (SIT)

7.6.1 The System shall be considered ready for UAT only if SIT meets the following:

a) Successful execution of the testable scenarios for operations;

b) Functional, Performance & Availability Requirements are met;

c) There is zero defect of Severity 2 and Severity 3 problems (refer **Annex 9.1**, section 4.2, for SLA definition); and

d) The number of outstanding Severity 4 defects is not greater than 20% of the total reported defect volume. (i.e. if in total there were 20 defects, there are not more than 4 Severity 4 defects outstanding).

7.7 User Acceptance Testing (UAT)

7.7.1 The System will be accepted and released for implementation only if UAT meets the following:

a) Successful completion of System Integration Testing;

b) Functional, Performance & Availability Requirements are met;

c) There is zero defect of Severity 2, Severity 3 problems (refer **Annex 9.1**, section 4.2, for SLA definition); and

d) The number of outstanding Severity 4 defects

- shall not be greater than 10% of the total number of UAT test cases and
- must be agreed by SATS to proceed for implementation move

7.7.2 In the event when the number of Defects in UAT exceeds 0.25 of the Defect Density (means “Defect Density = Number of Defect / Total Number of Test Cases”), SATS has the rights to call off UAT and request the appointed Vendor to re-do unit testing and SIT and rectify all defects before UAT is re-initiated. All such re-testing shall be conducted by the appointed Vendor at no additional costs to SATS.

7.7.3 The remaining 10% of the outstanding Severity 4 issues shall be resolved within one (1) month after Warranty Period starts. The appointed Vendor shall be subjected to service level credits (**Annex 9.1**, Section 4.4) in the event the outstanding Severity 4 issues are not resolved.

8 WARRANTY PERIOD

8.1 All Vendors shall quote for the following warranty options:

a) Twelve (12) months Warranty Period

b) Twenty four (24) months Warranty Period

The final warranty period shall be decided by SATS, at its sole discretion. This will begin from the date the system is deemed to be of satisfactory condition after receipt and acceptance by SATS.

8.2 The warranty shall cover labour for bug fixes and cost of any damaged labels due to printing faults during the stipulated period.

8.3 The appointed Vendor shall comply with the following during the Warranty Period:

a) Resolve 100% of Severity 2 and 3, 90% of Severity 4 of the functional and technical incidents raised, even if the resolution period extends beyond the warranty period.
b) The remaining 10% of the outstanding Severity 4 issues shall be resolved within one (1) month after Warranty Period ends. The appointed Vendor shall be subjected to service level credits (**Annex 9.1**, Section 4.4) in the event the outstanding Severity 4 issues are not resolved.
c) Maintain the list of post-implementation incidents/issues as well as resolutions.
d) Provide periodic statistical reports on the nature of the incidents/issues and service level.
e) Provide phone number for daily support coverage from 8.30am – 5.30pm.
f) Conduct weekly meetings to update on the status of all outstanding incidents.
g) Gather requirements for Change Requests raised during Warranty Period, and provide sizing of the effort, impact analysis; and implement the Change Requests upon approval by SATS. Troubleshoot interface problems with 3rd party interfacing systems and ensure problems are resolved
h) Work with relevant parties to investigate issues such as performance, hardware, OS, database, server software and other standard system software to resolve problems in the respective areas.

8.4 The appointed Vendor shall define clearly the proposed support structure to support the Warranty Period. The appointed Vendor shall provide resources and workflows in place to accept and manage incidents.

8.5 The incident management processes are shown in **Annex 9.2** (Service Level Agreement - Incident Management).

8.6 The support provided by the appointed Vendor during the Warranty Period shall adhere to the Service Level Agreement (SLA) as stipulated in **Annex 9.1** (Service Level Agreement during Warranty Period).

8.7 The Warranty Period shall commence only after the official sign off from SATS has been completed. Successful completion of the Warranty Period is subject to the fulfillment of the requirements stipulated in **Section 7** (Testing and Acceptance) and upon official sign off from SATS. Do note SATS reserves the right to request an extension of the Warranty Period in the event the stipulated requirements are not fulfilled. This shall be at no additional costs to SATS.

9 MAINTENANCE AND SUPPORT

9.1 The appointed Vendor should provide list of parts that are expected to wear and fail during daily usage, and to list local vendors for the replacement parts.

9.2 Where obtainable, the appointed Vendor should provide MTBF numbers for common wear and tear items such as wheels, gears, brakes and battery. This numbers can then be used to propose a schedule for preventive maintenance.

9.3 The appointed Vendor shall comply with requirement under **Annex 14** (Application Maintenance Services).

9.4 For components that may become obsolete in the next 5 to 8 years, the vendor shall propose a suitable obsolescence management plan to SATS. The cost of such a plan may be listed in the maintenance cost. Where necessary, a mid-life upgrade programme can be proposed subject to conditions acceptable to SATS.

9.5 The appointed Vendor shall propose a training plan to upskill staff with AGV control. A train-the-trainer package shall be proposed as part of this plan.

9.6 The appointed Vendor should propose a basic training package for keeping the AGV fit for daily operation such as charging/replacing its battery and spotting/identifying general faults.

9.7 The appointed Vendor shall respond within 24 hours or next working day from receipt of call ticket for workdays and Sundays/public holidays respectively. By response, it refers to a representative reporting on-site to assess the fault and provide a work-around solution. Extension of deadline may be sought through SATS' authorised representative.

10 PROJECT MANAGEMENT

10.1 The appointed Vendor shall take on sole responsibility of project management, deployment and handover activities. The appointed Vendor shall also be required to work and manage other vendors for interfaces development, testing and implementation (where needed by SATS).

10.2 The appointed Vendor shall ensure that SATS is provided with a full-time, qualified Project Manager to (including but not limited to):

a) Work with SFS Project Lead & SATS Technology Project Manager to manage and drive the end-to-end delivery of the project;
b) Work with SATS' I&T representative to request for and accept the required Development and Test environments for the appointed Vendor's implementation team;
c) Manage change requests, risks and issues;
d) Identify and align interdependent activities with all parties;
e) Track and update project schedule;
f) Provide regular updates on the progress of project; and
g) Comply with industry practices and standards for project management, infrastructure design and web development

10.3 If the appointed Vendor chooses to work with one or more partners, the management of these partner(s) shall be the sole responsibility of the appointed Vendor. The vendor shall be SATS's prime and single point of contact.

10.4 All Vendors shall furnish the project organization structure, escalation process and resumes of ALL key members (inclusive of the proposed Project Manager). SATS reserves the right to request for a change of resources.

10.5 Project Schedule

10.5.1 The appointed Vendor shall be responsible for delivering the project plan and ensuring compliance to the agreed timelines. This shall include (but is not limited to), the detailed end-to-end Work Breakdown Structure and schedule, the stakeholder management plan, change request management plan, project risks and issue logs. As a guide, the project plan shall include the following tasks (including, but not limited to):

a) Review of project deliverables by SATS
b) Unit Functional Testing, SIT, UAT, regression testing schedules
c) Training schedule, including user training before and after UAT
d) Preparatory work prior to UAT
e) Resolution of defects found during UAT
f) Development, testing and implementing of all interfaces systems and/or external systems and/or parties.
g) Support during implementation and Warranty Period

10.6 Project Deliverables

10.6.1 As part of the implementation, the following documentations shall be delivered (including but not limited to):

a) Plan & Analysis
- Preliminary Design Review (PDR) presentation after Contract Signature where the appointed vendor shall address how the project deliverables will be met
- Project organization structure, with defined roles and responsibilities
- Project plan and schedule for delivery of each of the requirements. It shall include task/activity, workshop schedule with proper resource assigned to each task/activity, and enabling on-going tracking of milestones, dependencies and critical paths of the project
- Project kick-off deck

b) Design

- Critical Design Review presentation after PDR where the appointed vendor shall show the details design of their proposed system,
- Overall/detailed Design document and Sign-off
- System Architecture
- Functional Specifications and Sign-off
- Test Plan and Sign-off

c) Build
- Test Plan, scenarios, results (covering Functional, Integration and Performance testing) and Sign-off
- Training Plan and Sign-off
- Training schedule and materials (both hardcopy and soft copy) and Sign-off
- User Guide/Manual and Sign-off
- Implementation plan, Check List and Sign-off
- Post Implementation Support Plan and Sign-off

d) Deploy
- System Administration Guide (if any) and Sign-off
- Application Maintenance Guide and Sign-off
- Installation and Configuration Guide and Sign-off
- Updated integration/technical landscape and Sign-off

e) Post-Implementation
- List of outstanding system issues/defects, impact analysis and severity categorization
- Updated Change Request Log with detailed requirements, man-effort sizing and Sign-off
- Post Implementation Review Report and Sign-off

f) All Phases
- Weekly Project Status Report
- Project Risk and Mitigation Plan

10.6.2 Do note that all documentations and deliverables (stated within the RFP or otherwise) remains property of SATS and that the final list of deliverables shall be approved by SATS.

Should there be non-conformance to the performance and/or business and/or technical requirements during development and/or SIT and/or UAT and/or Warranty Period, Vendors will be solely responsible for all costs associated with rectifying the above stated

ANNEX 16: PRICING TABLE

PRICING TABLE A: PROVISION OF THE SYSTEM

S/No	Description	Quantity	UOM	Price (SGD)		Remarks
				Unit	Total	
1	AGV 1 Unit including: Towing Jig for Pallet Jack Towing Jig Trolley					
2	Warranty Option A: 12 months					
3	Warranty Option B: 24 months					
4	Others (please state details within sub-section, if any)					
Total Cost (with Warranty – Option A)						
Total Cost (with Warranty – Option B)						

PRICING TABLE B: RECURRING COST OF THE SYSTEM

S/No	Description	Quantity	UOM	Price (SGD)		Remarks
				Unit	Total	
1	Maintenance and Support Option A: Daily (8.00am – 8.00pm)					
	Maintenance and Support for Year 1					
	Maintenance and Support for Year 2					
	Maintenance and Support for Year 3					
	Maintenance and Support for Year 4					
	Maintenance and Support for Year 5					
2	Maintenance and Support Option B: 24 hours x 7 days					
	Maintenance and Support for Year 1					
	Maintenance and Support for Year 2					
	Maintenance and Support for Year 3					
	Maintenance and Support for Year 4					
	Maintenance and Support for Year 5					
3	Others (please state details within sub-section, if any)					
Total Cost (with Maintenance and Support – Option A)						
Total Cost (with Maintenance and Support – Option B)						

Vendors to provide all details pertaining to the pricing for the submitted proposal, the validity shall be for a period of nine (9) months from the date of proposal.

All prices should be quoted in Singapore Dollars (SGD) and all prices are to exclude GST.

Should Vendors provide the product (software and hardware) in the form of License, SATS shall not own the Intellectual Property Rights except for customization.

Note:

- Should there be any additional items, please append the pricing table
- SATS will not be liable to incur any additional costs which is not listed in above
- The submission of Annex 16: Pricing Table is to be separated from tender proposals. Refer to section 3.3 for instruction of tender submission.

Payment Terms/Scheme

Vendors will follow the Payment Terms/Scheme as stated below (subjected to further changes by SATS):

Description	Amount
Upon signing of Formal Contract	10% of Quotation Amount
Upon sign-off of Detailed Design Specifications	30% of Quotation Amount
Upon acceptance of User Acceptance Test (UAT)	45% of Quotation Amount
Upon end of Warranty Period	15% of Quotation Amount
Total	**100% of Quotation Amount**

SATS and/or 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.

ANNEX 17: STANDARD CONTRACT

The Award of Tender shall be subject to such additional terms and conditions as may be agreed upon between SATS and the Vendors 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 in Figure 3 below:

Para. No.	SATS Standard Contract	Compliance	Remarks
1	Definitions and Intepretation		
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 6.4	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.

Figure 3: Sample of Compliance Table for Annex 17

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 17** (Standard Contract), in the table format shown in the figure above.

APPENDIX A (2): ENVELOPE LABEL FOR TENDER SUBMISSION

TO DEPOSIT INTO BLUE SATS TENDER BOX

Envelope Label:

Tender No: ***CT2010J020***

Tender Closing Date and Time: ***28 December 2020*** *– 12 NOON, SINGAPORE TIME*

Tender Description: *TENDER FOR* ***AUTONOMOUS GUIDED VEHICLE FOR SATS FOOD SERVICES PTE LTD***

Tender Conducted by: *SATS CENTRAL PURCHASING AND TENDERS MANAGEMENT (Tel No.: +65 65482080)*

TO:

SECRETARY TENDERS COMMITTEE (NON-FOODSTUFF & OTHER EQUIPMENT)
C/O SATS SECURITY ENTRANCE GATE
SATS INFLIGHT CATERING CENTRE 1
SINGAPORE 819659

FROM:

Name of Business Firm/Company:

Address:

Telephone and Fax Number:

Contact Person(s):