

CONFIDENTIAL



SATS TECHNOLOGY

Request for Tender

Project Title: Outdoor Hi-Lifts Video Analytics (VA) Phase 2

Tender Number: CT2103J003

Co. Regn No.: 198500562G

Confidentiality:

Do note that this Tender Document 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

TABLE OF CONTENTS 2

EXECUTIVE SUMMARY 3

INSTRUCTIONS FOR VENDORS..... 5

ANNEX 1: VENDOR PROFILE MATRIX 18

ANNEX 2: TENDER APPLICATION FORM 21

ANNEX 3: IPT DECLARATION BY VENDOR/CONTRACTING PARTY 23

ANNEX 4: INDIVIDUAL NON-DISCLOSURE AGREEMENT..... 24

ANNEX 5: TERMS AND CONDITIONS ON USAGE OF SATS IT RESOURCES 25

ANNEX 6: SAMPLE BANKER’S GUARANTEE..... 27

ANNEX 7: WSH RULES AND REGULATIONS..... 28

**ANNEX 8.1: SERVICE LEVEL AGREEMENT FOR WARRANTY PERIOD AND APPLICATION
MAINTENANCE SERVICES (AFTER WARRANTY PERIOD)..... 32**

ANNEX 8.2: SERVICE LEVEL AGREEMENT – INCIDENT MANAGEMENT 37

ANNEX 9: INFORMATION SECURITY REQUIREMENTS 43

ANNEX 10: INFRASTRUCTURE AND ARCHITECTURE STANDARDS 47

ANNEX 11: IT OPERATIONS STANDARDS AND GUIDELINES..... 50

ANNEX 12: SATS CODING PRACTICES 51

ANNEX 13: APPLICATION MAINTENANCE SERVICES..... 53

ANNEX 14: SCOPE OF WORK - DETAILED 56

ANNEX 15: PRICING TABLE 70

ANNEX 16: STANDARD CONTRACT 72

APPENDIX A (1): ENVELOPE LABEL FOR TENDER SUBMISSION 73

EXECUTIVE SUMMARY

1. ABOUT SATS

- 1.1. SATS is Asia's leading provider of gateway services and food solutions.
- 1.2. Our comprehensive Gateway Services encompass airfreight handling, passenger services, ramp handling, baggage handling, aviation security services, aircraft interior and exterior cleaning as well as cruise handling and terminal management. Our Food Solutions include airline catering, institutional and remote catering, aviation laundry as well as food distribution and logistics.

2. BACKGROUND

2.1. Automated and Centralized CCTV Footage Retrieval for Hi-Lift Operations

SATS Catering Cabin Hi-Lifts are all installed with CCTV systems. These CCTVs are used for incident investigation, audits and process, quality and safety compliance purposes. Hi-Lift CCTVs have proven to be an immensely valuable tool for SATS Cabin operations and are accessed with increasing frequency by Cabin staff to ensure conclusive investigation findings, and compliance reassurance to relevant stakeholders. However, the inherent inefficiency of physical footage retrieval becomes more apparent with the increasingly frequent access.

2.2. Trial of Video Analytics (VA) for Hi-Lift Operations

SATS Catering has explored the idea of using VA to aid in the process of incident investigations. Trials have previously been conducted in the form of retrieving physical footages from the Hi-Lifts and passing through a VA server whereby non-compliance of safety behaviour have been picked up. Initial results were accurate and encouraging for SATS Catering to further explore the idea of fully automating this end-to-end process of physically retrieving the footages and allowing the use of VA to alert Cabin staff of non-compliance in safety behaviour

3. PROBLEM STATEMENT

- 3.1. Decentralised self-contained Hi-Lift CCTV units resulted in inefficiency in footage retrieval operations. Cabin staff are required to physically access individual Hi-Lift's CCTV Video footage for manual retrieval of the physical CCTV storage device from the Hi-Lift and bring the storage device back for connection to a PC workstation that has specialized software installed, in order to view the CCTV footage data stored on that particular physical CCTV storage device. Cabin often finds itself requiring to install multiple specialized / proprietary-CCTV reader software due to the proprietary nature of the CCTV systems. In addition, during the retrieval process, the Hi-Lift will be left with an unserviceable CCTV unit due to the missing storage device in the CCTV Digital Video Recorder (DVR).
- 3.2. Conducting process, quality and safety compliance audits by manually combing through hours of CCTV footage is highly inefficient use of staff working time. The auditor's competency to pick up process irregularity varies from person to person as well which means the quality standards of audit could be undermined. The audit coverage is also limited by the available staff man-hours to go comb through the CCTV footage which means possible critical process discrepancies with potential impact to aircraft and personal safety goes undiscovered.

4. BUSINESS GOALS / OBJECTIVES

- 4.1. To develop an automated Hi-Lift CCTV footage retrieval system with a local centralised database server for CCTV footage archiving and management.

- 4.2. To develop a digital architecture to process the downloaded footage in the centralised database server for VA processing and notifications alert modules to sounds out potential irregularity and discrepancies.
- 4.3. Current implementation is for 35x Hi-Lifts vehicles. There will be a future full expansion to the rest of the fleet at a total final quantity of 100x Hi-Lifts vehicles (subject to the 35 HL implementation results)

5. BUSINESS BENEFITS

- 5.1. To increase operation efficiency by eliminating the need for physical access to CCTV footages by Cabin staff and eliminate the down time incurred on Hi-Lift due to unserviceable CCTV unit.
- 5.2. To increase audit / inspection efficiency, quality and maximizing audit coverage by automating the process using VA and aids quicker human intervention to manage uncovered irregularity and discrepancies.

INSTRUCTIONS FOR VENDORS

SECTION 1: DEFINITION OF TENDER DOCUMENTS

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

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

All Tender documents and clarifications shall form an integral part of a Contract that is to be entered into between SATS and/or its subsidiaries 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 Tender, will be issued accordingly as stated below:

- Annex 1 - Vendor Profile Matrix
- Annex 2 - Tender Application Form
- Annex 3 - IPT Declaration by Vendor/Contracting Party
- Annex 4 - Individual Non-Disclosure Agreement
- Annex 5 - Terms and Conditions on Usage of SATS IT Resources
- Annex 6 - Sample Banker’s Guarantee
- Annex 7 - WSH Rules and Regulations
- Annex 8.1 - Service Level Agreement
- Annex 8.2 - Service Level Agreement - Incident Management
- Annex 9 - Information Security Requirements
- Annex 10 - Infrastructure and Architecture Standards
- Annex 11 - IT Operations Standards and Guidelines
- Annex 12 - SATS Coding Practices
- Annex 13 - Application Maintenance Services
- Annex 14 - Scope of Work (Detailed)
- Annex 15 - Pricing Table
- Annex 16 - Standard Contract (“Contract”)
- Appendix A (1) - Envelope Label for Tender Submission

Do note that the Non-Disclosure Agreement (NDA) will be provided as a separate document.

SECTION 2: SCHEDULE OF EVENTS

EVENT	DATE
Tender Publication (Tender Release date)	26-Mar-2021
¹ Project Briefing	Date: 19-Apr-2021 Time: 2:00pm Venue: Inflight Catering Centre 2, Level 4 Contact Person: Lim Yong Jun Contact Number: 92956383
Questions from Vendors	19-Apr-2021 to 23-Apr-2021
SATS's Responses to Questions	26-Apr-2021 to 03-May-2021
² Submission of Proposal (Tender Closing Date)	14-May-2021, 12 Noon
Vendor Presentation (onsite at SATS Premises) - tentative	17-May-2021 to 21-May-2021
Appointment of Vendor(s)	Three (3) months from Submission of Proposal

¹ Refer to 3.2 Project Briefing

² Refer to 3.3 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: Lim Yong Jun
Email Address: yongjun_lim@sats.com.sg
Also CC to: 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) TENDER Reference Number: **CT2103J003**
- (2) Name of vendor;
- (3) Date of submission; and
- (4) Document Number e.g. CT2103J003, Vendor XXX, 06 Feb 2021, 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 ONE (1) representatives to attend the project briefing.

Attendees whose organization has not submitted the original signed NDA will not allowed to attend the project briefing.

Attendees are required to present 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 (3) sets of the Tender Submission, i.e. One (1) sets 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 8 (Pricing Table) is to be separated from tender proposals, i.e. One (1) sets original and two (2) sets of copies for Annex 8 (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 CT2103J003".

In addition, prepare TWO (2) (*Secure Digital*) SD Memory Cards containing the soft copy of your Tender Submission. Label the envelop containing the Digital Storage Devices (SD Cards) with the tender reference number, project name and your organisation's name; and mark the SD cards with the Tender reference Number: "CT2103J003

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 purpose, the cover of the document, please use the envelope label shown in Appendix A, MUST be clearly marked with 'Tender for Outdoor Hi-Lifts Video Analytics (VA) Phase 2 and the tender reference number CT2103J003.***

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.

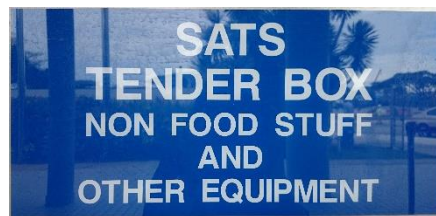


Figure 1: SATS Tender Box for Tender Proposals Submission

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.

Strictly no online or e-mail submission is permitted. 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 Tender 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 Tender process at any time and make no commitment, implied or otherwise, that the Tender 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 **Tender** does not commit SATS and its subsidiaries to pay for any costs incurred by Vendors in responding to this Tender, nor does it commit SATS and its subsidiaries to procure products and/or contract for services.

3.5.2 Terms of Applications

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.

If the Vendor is a corporation, the **Annex 2** (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 2** (Tender Application Form) is allowed.

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

3.5.3 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 submitted by the Vendor and filled in the space "TOTAL AMOUNT TENDERED" on the **Annex 2** (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.

3.5.4 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.

3.5.5 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.

3.5.6 Compliance to Requirements, Standards and Guides

Vendors shall comply with all business and technical requirements, standards and guides specified in the Tender unless otherwise stated in accordance with *Section 4: Format of Proposal, Part 5: 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

3.5.7 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.

3.5.8 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).

3.5.9 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 Tender.

3.5.10 Communications

After **the Tender** publication 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.

3.5.11 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 Tender submission, subjected to approval by SATS.

3.5.12 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.

3.5.13 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.

3.5.14 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.

3.5.15 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 6** (Sample Banker's Guarantee) must be complied with.

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

3.5.16 Payment Terms/Scheme

Vendors will follow the Payment Terms/Scheme in accordance with the payment milestones stated by SATS under **Annex 15** (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.

3.5.17 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 FOR 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.

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

Part 1: Non-Disclosure Agreement (NDA)

Enclose a copy of the duly signed NDA in this part.

No changes are allowed on the terms and conditions of SATS Non-Disclosure Agreement.

SATS and/or its subsidiaries reserve the right to share your response to the Tender with its advisors, if required.

Before commencing work for SATS and/or its subsidiaries, employees/subcontractors of appointed Vendors will also be required to sign “**Annex 4** (Individual Non-Disclosure Agreement)” and undertake to abide the “**Annex 5** (Terms And Conditions on Usage of SATS IT Resources)” if such employees/subcontractors of the appointed Vendor(s) are required to use SATS equipment.

Note: Vendors must have Non-Disclosure Agreement(s) with their sub-contractors.

Part 2: Vendor Profile Matrix

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

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

Do note that incomplete information could lead to disqualification.

Part 3: Tender Forms

Enclose within:

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

If the Vendor is a corporation, the **Annex 2** (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 2** (Tender Application Form) is allowed.

For **Annex 3** (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 4: 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 Tender.

Part 5: Proposed Solution

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

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 three (3) months' period, commencing from the date of system operational launch.

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

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

Part 6: Prior Experience

Vendors must provide extensive details of a minimum of two (2) projects, which they have relevant experience in. These must be similar to the nature of this Tender.

Part 7: Compliance Table

Provide a complete point-by-point response in ALL sections (i.e. Section 3 to Annex 16). 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 1	Vendor Profile Matrix
Annex 2	Tender Application Form
Annex 3	IPT Declaration by Vendor/Contracting Party
Annex 4	Individual Non-Disclosure Agreement
Annex 5	Terms and Conditions on Usage of SATS IT Resources
Annex 6	Sample Banker's Guarantee
Annex 7	WSH Rules and Regulations
Annex 8.1	Service Level Agreement
Annex 8.2	Service Level Agreement - Incident Management
Annex 9	Information Security Requirements
Annex 10	Infrastructure and Architecture Standards
Annex 11	IT Operations Standards and Guidelines
Annex 12	SATS Coding Practices
Annex 13	Application Maintenance Services
Annex 14	Scope of Work (Detailed)
Annex 15	Pricing Table
Annex 16	Standard Contract ("Contract")
Appendix A (1)	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 Tender requirement as written.

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

Figure 2: Sample of Compliance Table for Section 3 to Annex 16

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 16** (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 8: Pricing / Payment Terms

For work covered in this Tender, Vendors must submit a fixed fee proposal (provide price breakdown where possible) within the **Annex 15** (Pricing Table).

The submission of **Annex 15** (Pricing Table) is to be separated from Tender proposals, i.e. **Annex 15** (Pricing Table) are not to be filed or bind together with the 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 three (3) 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

CONFIDENTIAL

CT2103J003 – Outdoor Hi-Lifts Video Analytics (VA) Phase 2

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 twelve (12) months from the deadline for Submission of Proposal.

Vendors shall bear any withholding tax, if applicable.

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


ANNEX 1: VENDOR PROFILE MATRIX

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

Category/Section	Description		
Corporate Information			
Company's Name and Address (i.e. company bidding for this Tender)			
Year of Incorporation			
Parent Company Name and Address (if any)			
Mission and Direction			
Core Competencies / Business			
Technology / Business Partner			
Financial	2018	2019	2020
Revenue for the 3 most current year-end periods of company bidding for this Tender (in the currency of Singapore Dollars)			
Net Profit for the 3 most current year-end periods of company bidding for this Tender (in the currency of Singapore Dollars)			
Average Net Working capital amount (SGD)			
Revenue stream/order book/project pipeline (SGD)			
Fixed Overheads and committed (non-deferrable) SGD long term dues/payments/debts [excluding short term loans/debts]			
Short Term Loans (typically loans of less than 18 months duration) \$			
Financial Net Gearing Ratio: <small>(Short-term debt + Long-term debt + bank overdrafts + Capital leases) ÷ shareholders' Equity (%)</small>			
CAPEX to EBITDA Ratio: $CAPEX \div EBITDA$			
Payroll to Revenue Ratio			
Creditor Days = $(Accounts\ Payable \div cost\ of\ sales) * 365\ days$			
Debtor Days = $(Accounts\ Receivable \div annual\ credit\ sales) * 365\ days$			
Depreciation and Amortization charged (SGD)			
EBIT (earnings before interest & taxes) SGD			
Contact Person's Name, Job Title, email address, mobile & DID contact no., fax no.			

Category/Section	Description
Experience	
Relevant Project Experience - number of years - state the projects title (a brief description can be given as attachment)	
Gateway Services and/or Food Solutions Project Experience - state the projects title (a brief description can be given as attachment)	
SATS Project Experience - state the projects title (a brief description can be given as attachment)	
List three (3) relevant Customer References to this project, other than the references that have been stated above (no duplicate customer references) - number of years - state the project title (a brief description can be given as attachment)	
Product Features	
Product Overview	
Technology Platform (e.g. DotNet, J2EE, C etc.)	
Client (e.g. browser-based, Java client, etc.)	
Server (e.g. Windows, Unix, etc.)	
DBMS (e.g. Oracle, SQL*Server, etc.)	
Interfaces Supported (e.g. MQ-Series, Web Services etc.)	
Years in Market	
Estimated Market Share	
Resources	
Number of Staff Worldwide - Total - Technical (Consultant, Engineer, etc.) - Post Implementation Support	
Number of Staff in Singapore	

Category/Section	Description
<ul style="list-style-type: none">- Total- Technical (Consultant, Engineer, etc.)- Post Implementation Support	
State the number of staff and the total number of years for each technology skill set / design standard in: Web Design J2EE DotNet Web Services Weblogic MQ-Series or equivalent Oracle 10g and above SQL Server RF Technology Others (please specify)	
Project Management	
Development Methodology Adopted	
Development Model (on-site/off-shore/ hybrid)	
CMM, ISO or equivalent Certification	
Information Security and Quality Assurance	
State whether your organisation has a series of documented Information Security policies and Quality Assurance policies. Existing Information Security policies (Yes / No) Existing Quality Assurance policies (Yes / No)	

	ANNEX 2: TENDER APPLICATION FORM	TENDER NO: CT2103J003
DESCRIPTION: Outdoor Hi-Lifts Video Analytics (VA) Phase 2		
TENDER CLOSING DATE & TIME: 14-MAY-2021 1200 Noon Singapore time	Upon submission of Tender, the Vendor shall be deemed to have accepted unconditionally and without qualification all the terms and conditions in the Tender Documents. Manager, Central Purchasing and Tenders Management	
TENDER VALIDITY: UNTIL TWELVE (12) MONTHS FROM TENDER CLOSING DATE TENDER AMOUNT:		
VENDOR'S FULL BUSINESS/CORPORATE NAME AND ADDRESS		
VENDOR'S GOODS AND SERVICES TAX REGISTRATION NO: <i> Please state "NA" if not applicable.</i>		
VENDOR'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 Vendor, 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 twelve (12) 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.

Vendor's business/company stamp

Signature of Vendor or its authorised signatory

Full Name and Designation of Vendor's authorised signatory

Date

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

ANNEX 3: IPT DECLARATION BY VENDOR/CONTRACTING PARTY

DECLARATION BY VENDOR / CONTRACTING PARTY

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

I/WE, , hereby declare that:
(Name of Vendor / 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 4: 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 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:
Designation:
Date:

Name:
Designation:
Date:

ANNEX 5: 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. endeavour to strictly comply with SATS’ security policies when using or accessing SATS’ IT resources including but not limited to, e-mail, intranet, and applications.
 - b. protect the confidentiality of the PIN(s) or password(s) assigned to him/her at all times and ensure that the same is not revealed or disclosed in any manner whatsoever to any person or persons whomsoever, within SATS or outside.
 - c. use the IT resources strictly for official company business only, and will be responsible to ensure that resources will be used for the purpose intended for.
 - d. acquire, install and use licensed and 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.

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

[For employers only] SATS reserves the right to request the removal of any of your employee from the Project team forthwith and/or terminate the Agreement forthwith if you or any employee or subcontractors or agents commits a breach of or is in non-compliance with any provision of these T&Cs. Should SATS request the removal of such employee, you will endeavour to procure a replacement. Any such replacement offered by you shall be subject to SATS' prior written consent, which consent shall not be unreasonably withheld.

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

(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] 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 6: SAMPLE BANKER'S GUARANTEE

[insert date]

SATS Catering Pte 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 7: 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.

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.

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

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.

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.

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.

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

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

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

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

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

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

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.

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.

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

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.

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

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

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.

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

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.

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

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

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

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.

7.0 Ladders

7.1 The contractor is required to provide his or her own ladders, with company identification clearly

8.6 Dual Flashback 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 safely 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 In-house 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 where 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 CATERING PTE LTD** 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 8.1: SERVICE LEVEL AGREEMENT FOR WARRANTY PERIOD AND APPLICATION MAINTENANCE SERVICES (AFTER WARRANTY PERIOD)

1. MAINTENANCE SUPPORT & HELPDESK HOURS

Provide 24 hours x 7 days maintenance support and helpdesk hours:

- Option A - For Sev 2 (High) maintenance support.
- Option B - For Sev 3 (Medium) maintenance support

2. INCIDENT MANAGEMENT

Vendors will need to comply with SATS's incident management flow (refer to **Annex 8.2** (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 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)		Workaround Time	Resolution Time (To produce Resolution)
	Critical	Non-Critical	Widespread	Localised	Major	Minor	Yes	No	Office Hours	Out of Office Hrs		
Critical	X		X		X			X	30 min	2 hours	2 hours	2 hours
High	NA			X	X			X	60 min	60 min	2 hours	> 95% within 6 hours Residual within 24 hrs
		X	X		NA			X				
Medium	NA			X		X		X	4 hours	Next working day	1 working days	> 95% within 3 working days Residual within 5 working days
Low	NA			X		X	X		1 day	Next working day	5 working days	> 95% within 10 working days Residual within 12 working days

Note: The above mentioned SLA is applicable for this project only

4.2 DEFINITIONS OF SEVERITY LEVELS

<u>Severity Level</u>	<u>Description</u>
Critical	An Incident or Problem shall be assigned as “Severity Level-Critical” if: <ul style="list-style-type: none"> • The Incident or Problem causes or will potentially cause Major Business Impact, which affects a Widespread User Base.
High	An Incident or Problem shall be assigned as “Severity Level-High” if: <ul style="list-style-type: none"> • 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.
Medium	An Incident or Problem shall be assigned as “Severity Level-Medium” if: <ul style="list-style-type: none"> • The Incident or Problem causes or will potentially cause Minor Business Impact; and • There is no Acceptable Workaround for the Incident.
Low	An Incident or Problem shall be assigned as “Severity Level-Low” if: <ul style="list-style-type: none"> • 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

<u>Term</u>	<u>Definition</u>
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 organization 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.
Localized	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, i.e. 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 High (2)	3
Severity level Medium (3)	2
Severity level Low (4)	1

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

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

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

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

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

Maximum SCUs = Total SCUs in a particular period, which is [6] (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	99.95%	Actual Downtime – Planned Downtime Allowed (15% of Monthly Transaction Fee) Subject to maximum amount
Transaction Response Time	98% of the transactions 3 to 5 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 = $\frac{\text{Total Time} - \text{Scheduled Outages} - \text{Unscheduled Outages}}{\text{Total Time} - \text{Scheduled Outages}} \times 100$
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	<u>ASP</u> : 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. <u>Blackbox/Whitebox</u> : Time taken from the moment an input message reaches the Application until the output is delivered from the Application.

ANNEX 8.2: 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 Incident Tickets (Severity Critical & High), 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 Incident Tickets (Severity Critical & High), 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 Incident Tickets (Severity Critical & High), 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 Incident Tickets (Severity Critical & High), 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 (i.e. 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

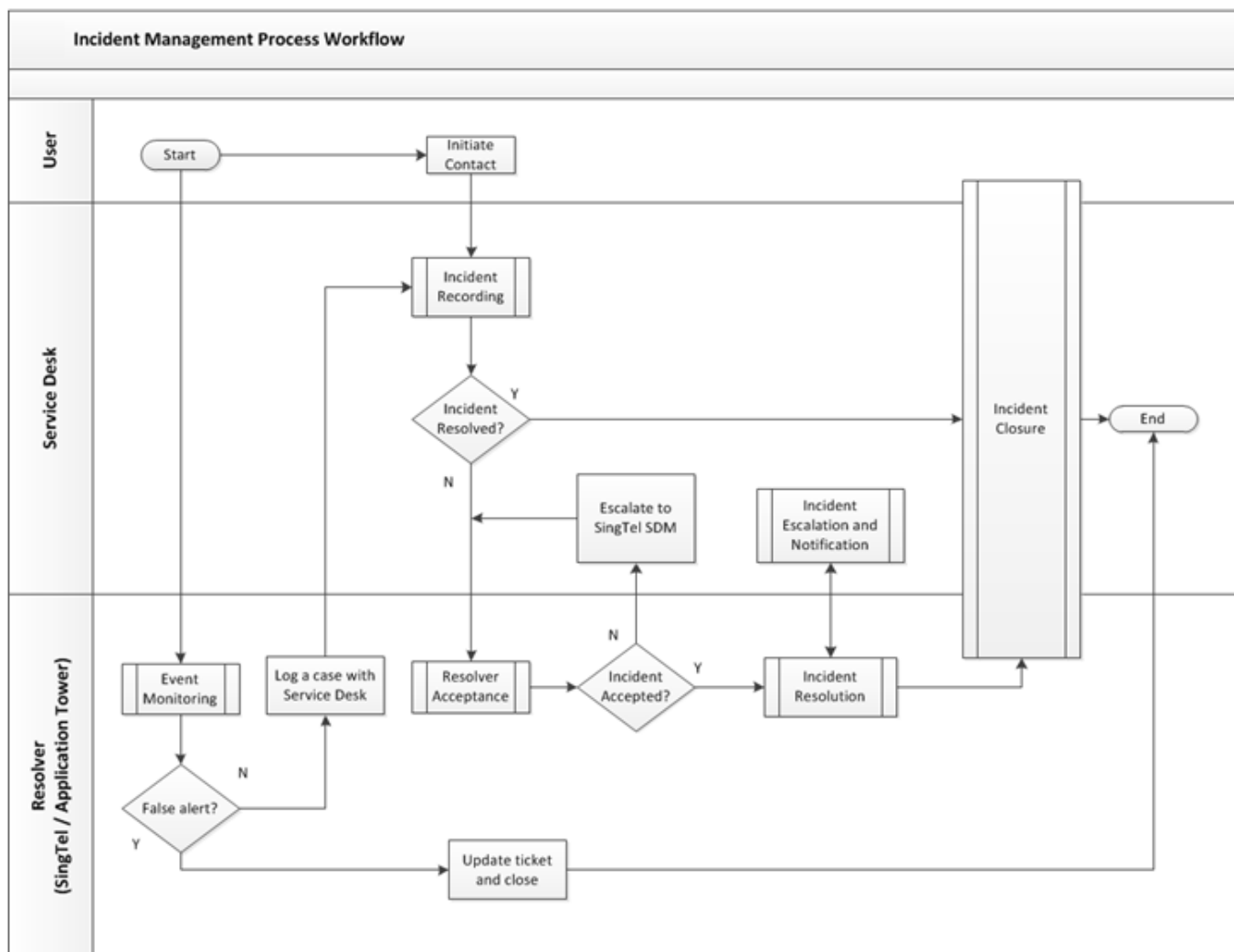
1. Contacts the User to discuss any outstanding issues regarding the incident.
2. Resolves incident and updates the incident ticket with the details of incident resolution.
3. Updates incident ticket with resolution details if ticket is transferred back by SMITH due to lack of resolution information 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 with the status 'Resolved' and Close the incident once the vendor resolved the incident.

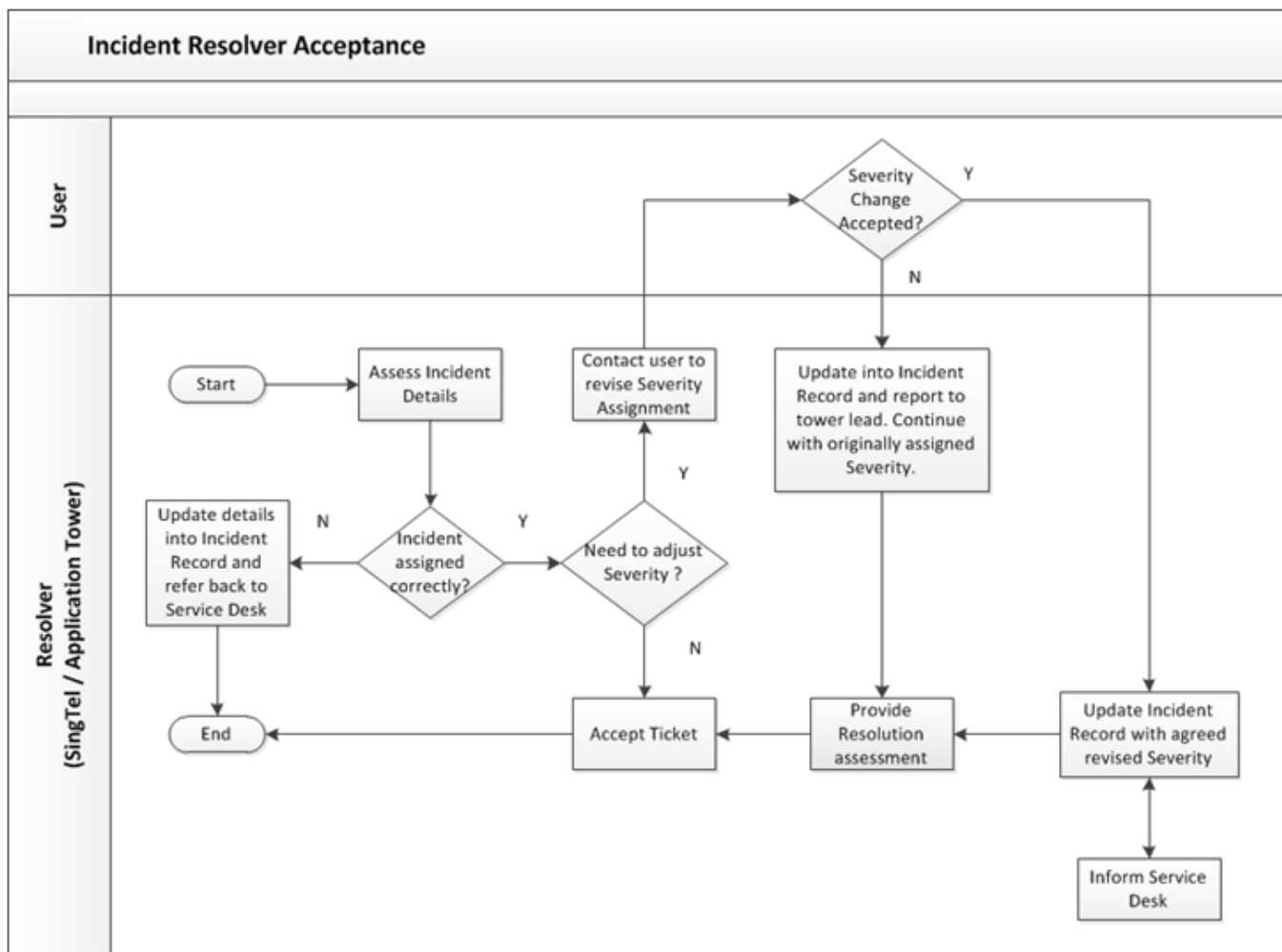
Note: Resolution details should be acceptable in order to go with incident closure. List down the steps/actions taken to solve

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.

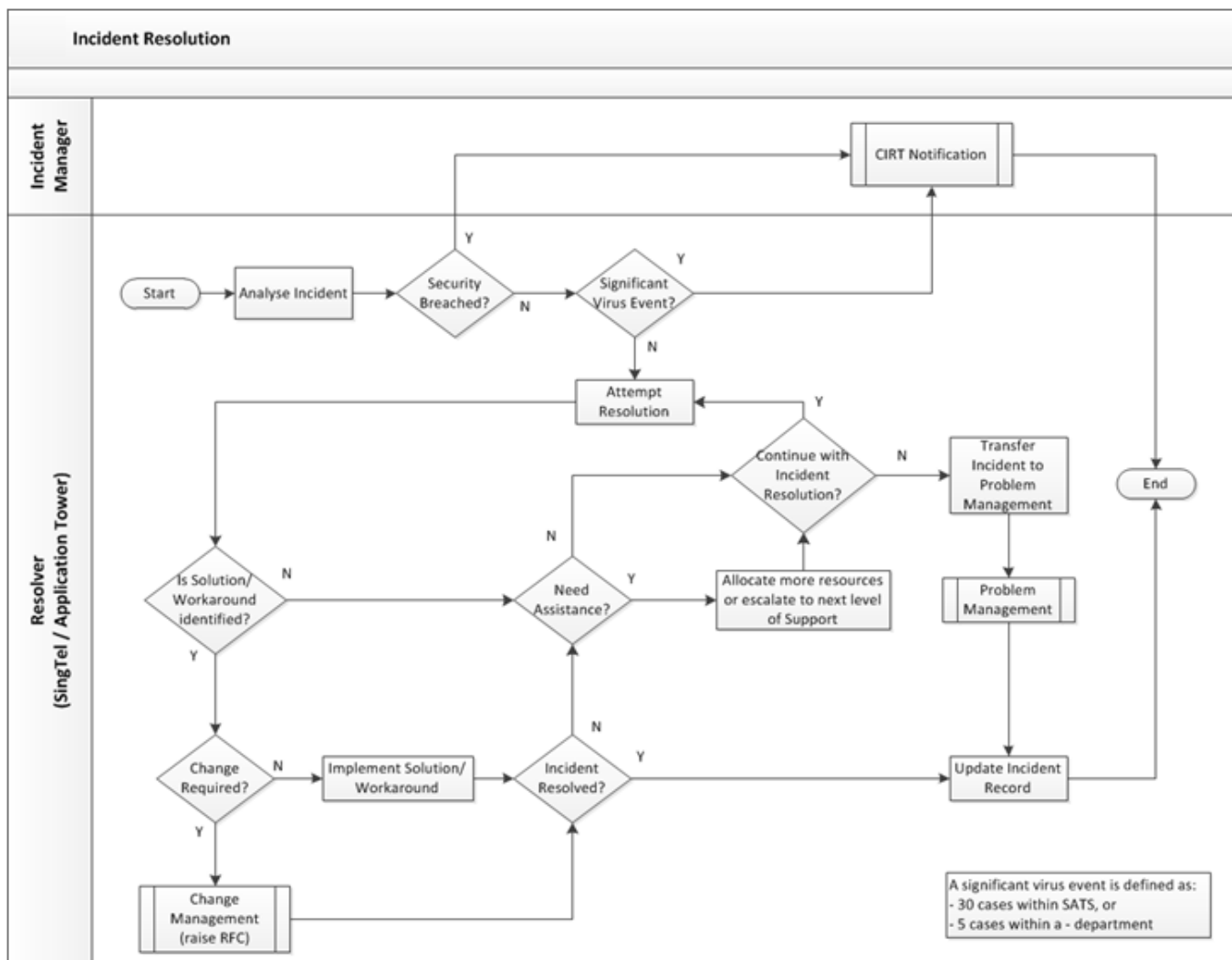
INCIDENT MANAGEMENT PROCESS OVERVIEW



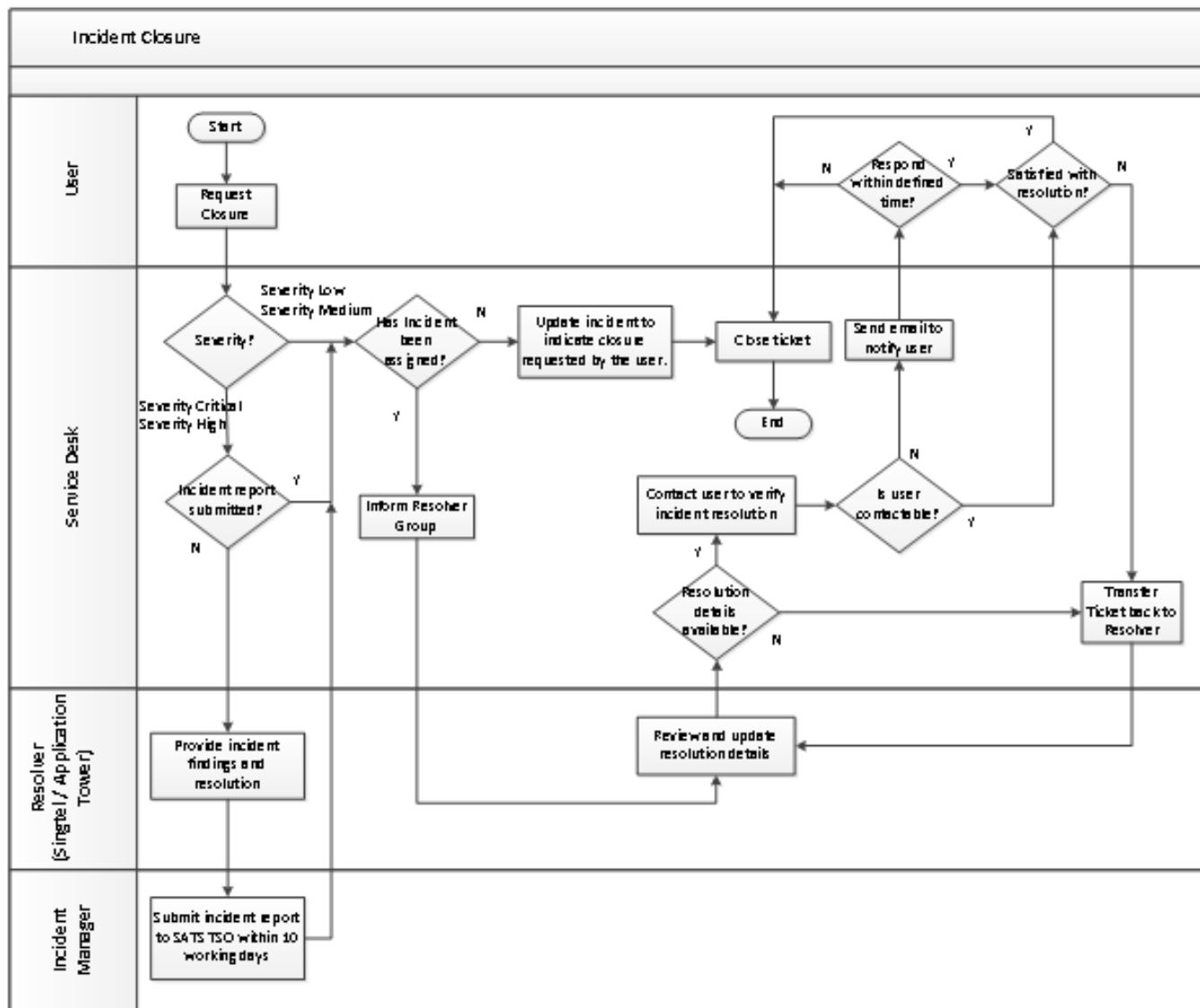
RESOLVER ACCEPTANCE PROCESS



INCIDENT RESOLUTION PROCESS



INCIDENT CLOSURE PROCESS



ANNEX 9: 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, attempts or has any possibility to breach the security of SATS' systems shall not be installed.
- 1.8 Implements processes and solutions to ensure protection against malicious attacks.
- 1.9 Personal computing devices not issued by SATS shall not be connected to SATS' resources unless explicit approval has been granted. Such approvals shall be temporary with a stated end date.
- 1.10 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 personal firewall and anti-virus software with up-to-date virus definition files before connecting to SATS' resources.
- 1.11 Protection of assets, including:
 - 1.11.1. Procedures to protect SATS assets, including data, hardware and software;
 - 1.11.2. Procedures to determine whether any compromise of the assets has occurred;
 - 1.11.3. Controls to ensure the return or destruction of data and assets at the end of, or at an agreed point in time, during the contract; and
 - 1.11.4. Restrictions on copying and disclosing information.
- 1.12 Responsibility with respect to legal matters including but not limited to the following:
 - 1.12.1 Subject to the Cybersecurity Act 2018 and/or any relevant law within and outside Singapore.
 - 1.12.2 Data, patent, copyright and privacy protection legislation
 - 1.12.3 Intellectual property rights and copyright assignment and protection of collaborative work.
- 1.13 Non-disclosure of information including but not limited to the following:
 - 1.13.1 Discovery of any security weakness shall not be disclosed to third parties, and shall be reported to SATS immediately;
 - 1.13.2 The Vendor shall not disclose to third parties, whether directly or indirectly, information regarding SATS' network, details of the applications or other information that they may have access to during the course of contract with SATS.
- 1.14 Compliance with a specified process for change management.

CONFIDENTIAL

- 1.14.1 Changes to production systems must be documented, reviewed, 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 shall be updated to reflect the changes.
- 1.15 Obtain approval and clearance from SATS before the Vendor appoints subcontractor(s) to support SATS' scope of work defined in the contract.
- 1.16 Obtain prior written approval from SATS before using SATS project work as a reference.
- 1.17 Submit an annual audit report, certified by the Vendor's auditors, on the services provided to SATS.

Security Incident Management

- 1.18 Submit an annual audit report, certified by the Vendor's auditors, on the services provided to SATS.
- 1.19 Handling of security incident:
 - 1.19.1. Immediately report any security incident involving their systems, and/or SATS resources to SATS' contact person and the Computer Incident Response Team (CIRT), and cooperate with the investigation as required.
 - 1.19.2. Ensure availability of services is maintained and take responsibility for the security incident.
 - 1.19.3. Provide logs in its native format without any alteration when requested.
 - 1.19.4. Provide an Investigation Report detailing the cause of the security incident and action done.

Logs Management

- 1.20 All logs shall be centrally stored and secured for possible forensic use. These would include but not limited to servers, routers, databases, intrusion detection system, firewalls, and application audit trail and access logs.
- 1.21 Audit logs shall include sufficient information to establish what events have occurred, who or what has caused them, and when did the events happened.
- 1.22 Establish procedures and processes for the monitoring and review of audit logs and the prompt reporting of security-related violations such as intrusion detection, unauthorised access or modifications. Such procedures and processes shall be documented, reviewed and updated regularly

Disaster Recovery

- 1.23 Dedicated to disaster recovery (applicable to hosting services):
 - 1.23.1. Availability of hot-site facilities
 - 1.23.2. Annual performance of recovery tests
 - 1.23.3. Back-up procedures in place.

Access Management

- 1.24 Limitation of access to SATS' business information to authorized personnel supporting SATS' systems, and access must be restricted to authorized areas and granted based on valid business need only.
 - 1.24.1 Physical and logical access controls to be put in place to restrict and limit access;
 - 1.24.2 Third parties shall not be allowed to access SATS' resources and network through the Vendor's network;
 - 1.24.3 Use of network sniffing tools is prohibited unless authorized by SATS;
 - 1.24.4 Permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;
 - 1.24.5 Establishment of an authorization process to authenticate all access, including users and administrators, to SATS resources;
 - 1.24.6 Maintenance of an authorized user list and what their rights and privileges are with respect to each account.
 - 1.24.7 Access by the Vendor's personnel/subcontractors/agents to SATS systems must be reviewed periodically to ensure currency of those personnel/subcontractors/agents and their access rights.

- 1.24.8 The Vendor must immediately notify SATS when account is no longer required.
- 1.24.9 Privileged account access must not be shared. All users requiring privilege access must have unique user IDs and owned individually.
- 1.24.10 All privileged access and activities must be logged. The log files and audit trails must be protected to facilitate future audit and investigations. The retention period of logs and audit trails need to comply with legal and regulatory requirements.

Application Security

- 1.25 System shall be developed based on a Three-Tier Architecture, separating the presentation tier, functional/business logic, and the database.
 - 1.25.1 Each tier shall be separated with a physical/virtual firewall and has only one (1) egress and/or ingress connection to the neighbouring tier.
 - 1.25.2 Connectivity between each tier shall be restricted to the following structure:
Presentation tier – Functional/business logic tier – Database
- 1.26 Application interfaces between systems shall be secured prior to transmitting information classified as CONFIDENTIAL or above. Examples of secure channel include, but not limited to SFTP, SSL and IPsec.
- 1.27 Vendor shall perform Vulnerability Assessment and Penetration Test before System Production Launch or deployment of any major change¹.
- 1.28 Vendor shall provide to SATS reports each detailing the performance of Vulnerability Assessment and Penetration Test, including the vulnerability identified and targeted remediation date.
- 1.29 All vulnerabilities identified from Vulnerability Assessment and Penetration Test must be remediated and approved by SATS before production launch or deployment of major change.
- 1.30 Internet-facing applications shall allow HTTPS only

Mobile Application Security

- 1.31 Vendor shall ensure mobile application is compatible to SATS Mobile Device Management (MDM) solution prior to deployment;
- 1.32 Vendor shall borne cost of effort, if required, to secure connectivity and communication between mobile application and server through SATS MDM.
- 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; and
 - 2.5 Know the Vendor's external connectivity to other networks, and how the segment to be used for SATS is protected.
 - 2.6 Vendors providing payment related services to SATS must comply with the guidelines published by Payment Card Industry (PCI) Security Standards Council at <https://www.pcisecuritystandards.org/> during the term of the Contract. The payment related services include activities that require the Vendor to store, process or transmit payment cardholder (e.g., credit card) data. The Payment Card Industry Data Security Standards ("PCI DSS") is a multifaceted security standard intended to protect payment cardholder data.

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.

- 2.7 The Vendor shall undertake the required validation procedures according to their Service Provider Level, and provide to SATS the equivalent reports that they are required to submit to the payment brands or acquiring banks based on their Service Provider Level. The Vendor shall indemnify SATS for any security breach resulting in loss or misuse of credit card data due to Vendor's non-compliance of PCI DSS.

ANNEX 10: INFRASTRUCTURE AND ARCHITECTURE STANDARDS

The standards listed shall be applied in the purchase and management of technologies and infrastructure that underpins SATS application systems and services.

The infrastructure and architecture standards do not describe what is currently supported in SATS environment, but solutions proposed by the Vendors need to minimally meet the stated standards in this Annex under the relevant section(s).

1. Desktop/Notebook Client Environment

- Microsoft Windows 7 SP1, Windows 10 Enterprise and above
- Internet Explorer 11 and above, latest version of Chrome and Firefox
- Endpoint Protection Security.
- No local administrator rights – All client applications, including associated components, must not be able to execute with local administrator rights.
- Client software distribution using MSI format run in silent mode

2. Handheld Client Environment

- Samsung A5
- Samsung Active Tab 2
- Samsung Gear S3

3. Server Environment (On-Premise)

- Operating System
 - Solaris 10 or later
 - AIX 7.1 or later
 - Windows Server 2016
 - Linux Red Hat Enterprise 7.5 and above
- Internet facing web server: Apache HTTP Server 2.2 or later
- Application Server
 - J2EE Application Server: BEA Weblogic 12c or later
- Messaging Software: MQSeries 7.5 or later
- Transactional Database
 - Oracle 11g Rel 2 or later
 - MS SQL Server 2016
 - Transactional Database Reporting Tool: Business Objects XI or later

4. Server Environment (Cloud)

- Conforms to the Infrastructure, Architecture and Standards of Cloud Provider.
- Vendor shall follow the SATS standard Cloud Architecture for the application as specified in Figure 3 (subjected to the approval of SATS), including but not limited to Azure, IaaS and PaaS
 - Production and UAT environment shall be separated without any inter-connectivity with each other
 - Each environment shall implement a 3-tier architecture, each in its own private subnet, consisting of Web, Application and Database tier respectively
 - Connectivity between each tier shall be in accordance with Annex 9 clause 1.25.
 - A public subnet hosting proxy and other related internet services shall be in place as the only interface between web tier and public access.

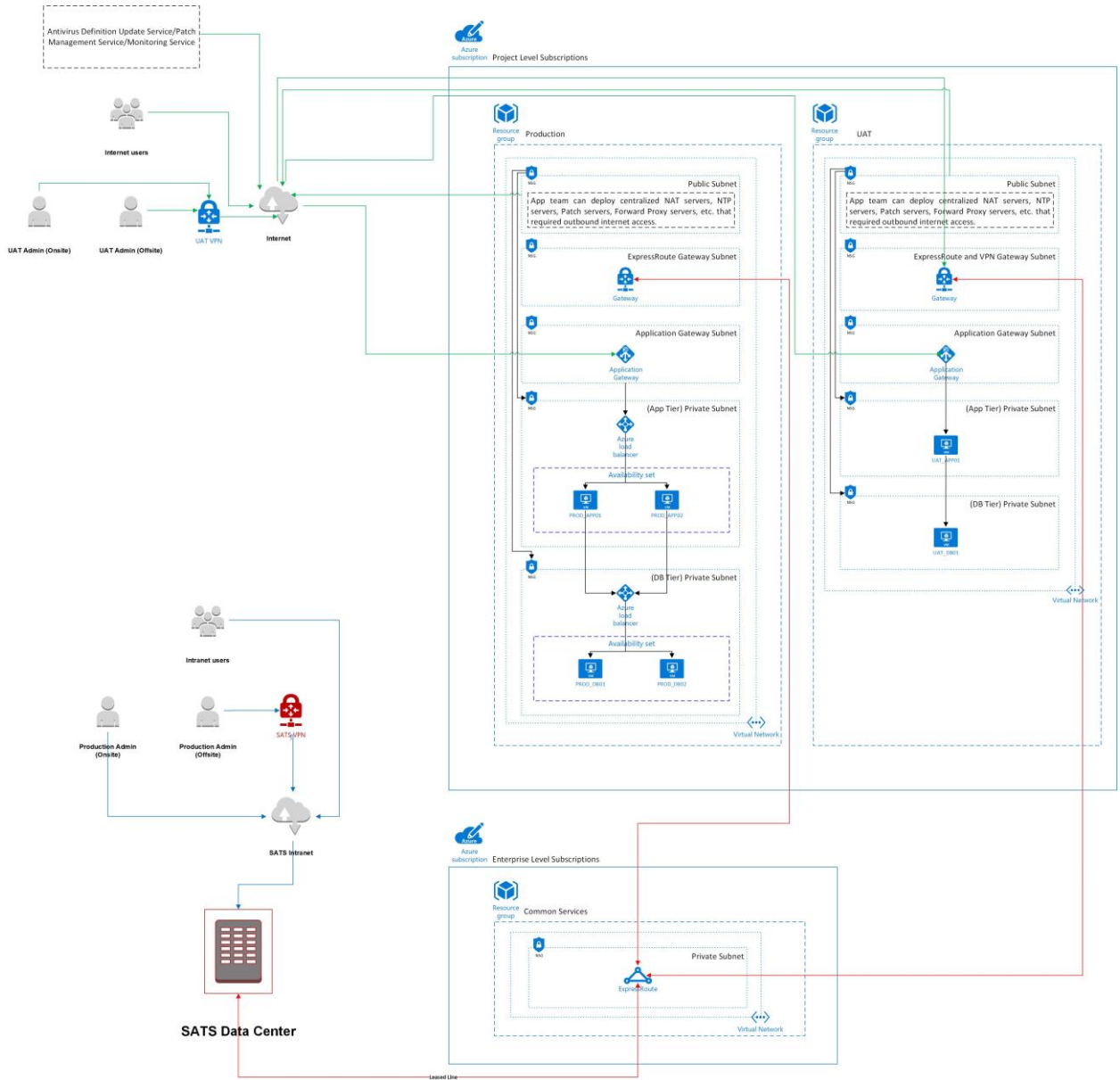


Figure 3 – SATS Standard Cloud Architecture

5. Connectivity

- Wireless – All clients connecting to Sats wireless infrastructure is required to support the IEEE 802.1X authentication method.
- Remote Access – Remote access, subjected to Sats approval, must be through client-to-site VPN with two factor authentication (2FA)

6. Authentication

- Active Directory Federation Services (ADFS) - Sats uses Windows Active Directory (AD) as its directory services and implemented Active Directory Federation Services (ADFS) to provide a platform for single sign-on access to systems and applications. Vendor is required to adopt ADFS in their solutions for authentication.

7. File Exchange

- File exchange between systems must use SFTP (SSH File Transfer Protocol).

8. Middleware

8.1. Asynchronous Services:

- a. All new asynchronous services must be built on the JMS open standards. SATS currently uses IBM MQ to support external asynchronous communication between SATS applications and other systems.
- b. All new asynchronous services must support the publish & subscribe model and dedicated point-to-point queue model.

8.2. Batch File Services:

- a. All batch files must be managed centrally and distributed centrally.
- b. All applications that produce a batch feed must send the output file to a centrally managed file server for distribution to third-party or downstream consuming applications. The application must be able to push the batch feed to the centrally managed file server or left in a local file system for the centrally managed file server to pull the feed to its internal storage.
- c. All applications that need to consume a batch feed from a third-party provider or an internal up-stream application must get the file from a centrally managed file server. The application must allow a batch feed to be able to push from the centrally managed file server to its local file system or pull the feed from the centrally managed file server.

9. Components

The Vendor's responsibilities include:

- (i) Unless otherwise directed by SATS, ensuring that the Software is supported by the IFS Software at the version (the "N" release level) stated within.
- (ii) As directed by SATS, also ensuring that the Software is supported by the release N-1 and earlier versions of the IFS Software for the longer of:
 - (a) The thirty-six (36) month period following version N's general public availability.
 - (b) The time the IFS Software vendor ceases to support such version.
- (iii) Using commercially reasonable efforts to maintain the Software that is no longer supported by the IFS Software vendor.

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

Note:

"IFS Software" refers to all items stated within.

ANNEX 11: 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(s) 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 (e.g. Rollforward_XXX_68.sh/rollback_XXX_68.sh for application XXX and the server is capsp68).
- 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 BMC Patrol.

ANNEX 12: 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 text 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. Error Handling

- 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. Logging

- 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. General Coding Practices

- 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 13: 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/software in client PCs that are required.

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. For onsite development and support, SATS will provide the necessary hardware and required software. In all cases, the Vendor is required to adhere to the Infrastructure and Architecture Standards as shown in Annex 10 (any deviations must be approved by SATS).

3.4. 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 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.

3.5. The Vendor is required to use SATS's management tools for (includes but not limited to): (1) source code, (2) problems, (3) changes and (4) configurations. Do note that no other management tools used and/or proposed by the Vendor will be used.

3.6. * 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.

3.7. The Vendor is required to meet the SLA for application maintenance services as shown in Annex 8.1 Service Level Agreement for Warranty Period and in Annex 13 Application Maintenance Services (After Warranty Period).

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

- 3.9. 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.
- 3.10. 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.
- 3.11. 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.
- 3.12. The Vendor is required to adhere to SATS's Information Security Requirements as shown in Annex 9, in all circumstances.
- 3.13. For offshore and off-site development and support, the Vendor may be given limited and restricted access to SATS network as specified in Annex 9 (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.
- 3.14. For 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 14: SCOPE OF WORK - DETAILED

1. Project Overview and Background

1.1 Automated and Centralized CCTV Footage Retrieval for Hi-Lift Operations

SATS Catering Cabin Hi-Lifts are all installed with CCTV systems. These CCTVs are used for incident investigation, audits and process, quality and safety compliance purposes. Hi-Lift CCTVs have proven to be an immensely valuable tool for SATS Cabin operations and are accessed with increasing frequency by Cabin staff to ensure conclusive investigation findings, and compliance reassurance to relevant stakeholders. However, the inherent inefficiency of physical footage retrieval becomes more apparent with the increasingly frequent access.

1.2 Trial of Video Analytics (VA) for Hi-Lift Operations

SATS Catering has explored the idea of using VA to aid in the process of incident investigations. Trials have previously been conducted in the form of retrieving physical footages from the Hi-Lifts and passing through a VA server whereby non-compliance of safety behaviour have been picked up. Initial results were accurate and encouraging for SATS Catering to further explore the idea of fully automating this end-to-end process of physically retrieving the footages and allowing the use of VA to alert Cabin staff of non-compliance in safety behaviour

2. Functional Requirements

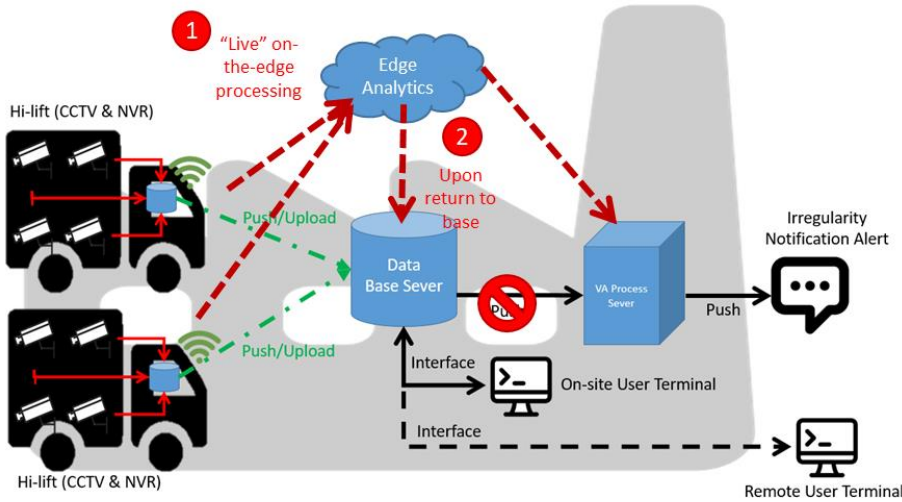
2.1 As-Is Business Workflow:

Current workflow is entirely manual. There is no VA used to detect non-compliant of safety behaviour. Any incidents are investigated post-happenings. Retrieval of footage from Hi-Lifts will be done and Cabin staff will painstakingly review through the footages to see if the actual incident is captured by the CCTVs. This would be followed by checks on the staff who were on duty during the time of incident and interviews would be conducted to find out more details

2.2 To-be Business Workflow (2x options to be proposed by vendors):

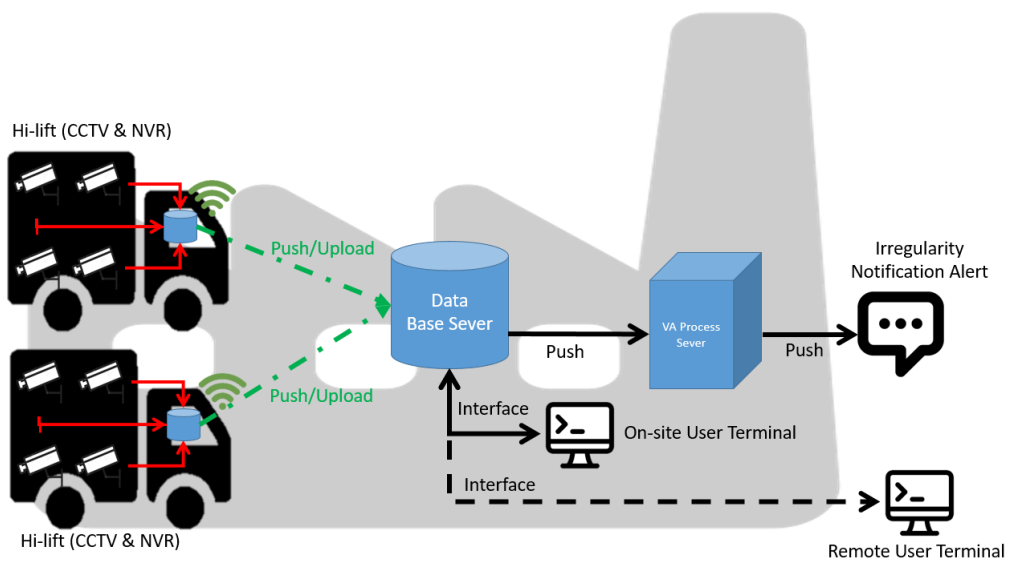
Option 1

Individual Hi-Lift CCTV footages are captured and recorded on the onboard Hi-Lift CCTV NVR unit. Instant edge-processing of the VA use-cases are performed "live". Any violations / irregularities / discrepancies from the default SOP will be flagged out and notified to the preselected addressess for the business unit to follow up and management measures. Upon returning to the Hi-Lift operational base and Wi-Fi connection is authenticated and established between the Hi-Lift and the local Wi-Fi network, the NVR will upload all the footages into the local database sever for storage purpose. The CCTV footages from all the Hi-Lifts stored in the proposed local database sever can be accessed by the user via a PC terminal on site or remotely.



Option 2

Individual Hi-Lift CCTV footages are captured and recorded on the onboard Hi-Lift CCTV NVR unit. Upon return to the Hi-Lift operational base and Wi-Fi connection is authenticated and established between the Hi-Lift and the local Wi-Fi network, the NVR will upload all the footages into the local database sever. The CCTV footages from all the Hi-Lifts stored in the proposed local database sever can be accessed by the user via a PC terminal on site or remotely. The CCTV footages stored in the database will be further automatically proceed to undergo VA software developed by the VA developer and any irregularities and discrepancies are flagged out and notified to preselected addressess for the business unit follow up and management measures.



2.3 New Business Requirements

2.3.1 CCTV NVR on Hi-Lift (for 35x vehicles)

- a) 4 network camera per Hi-Lift with option to interface with 8 cameras
- b) NVR
- c) Onboard storage 31 days' worth of footage
- d) Wi-Fi module to allow connection to S@TSWiFi and wireless transfer of videos

2.3.2 Local Database Sever

- a) Storage size to archive 95 days' worth of footage
- b) Storage build with robustness and resistant to network outage, trips and corruption into design consideration.

2.3.3 User Terminal

- a) Interface with the database sever to review, manage the footages stored with on-site and remote interface capability.
- b) Unified interface able to retrieve the footage across all the HL uploads

2.3.4 VA Protocol sever

- a) Process all footages push from the database and ran the predetermined VA protocols
- b) Generate timely reports on Irregularity/Discrepancies

2.3.5 VA Use-Cases

1. Verification of harness was donned during the aircraft cabin door opening and closing
2. Verification of lifeline attachment onto the harness worn by staff during the aircraft cabin door opening and closing
3. Verification of double stacking of containers and items on meal carts
4. Verification of Hi-Lift Platform Hand Rails deployment during cabin loading and unloading process
5. Verification of correct marshalling technique used by marshaller during marshalling of Hi-Lift in docking operations
6. Verification of circle of safety checks during Hi-Lift docking operations
7. Verification of Frisking of Door during aircraft cabin door closing
8. Self-diagnosis of Hi-Lift CCTV tampering

2.4 Reporting Requirements

2.4.1 Irregularity / Discrepancies Report

A summary of all Irregularity / Discrepancies identified by the VA sever module shall be generated and push in the form of MS Excel file via electronic mail to selected addresses. Parameters of the report, i.e. HL, date, time, type of irregularity / discrepancies, etc., shall be determine by the user. The frequency of the summary could be set by user in the interval ranging from hourly to daily depending on the level of criticality of the Irregularity/Discrepancies picked up by VA.

The User retain the ability to manage the notification addressees without seeking developer intervention.

2.5 Integration and Interfaces

2.5.1 N.A.

2.6 Dashboard

2.6.1 To have an online dashboard for status, alerts and exceptions

2.7 Vendor shall submit regular "Billing Reports" with the following data fields: Full Name of the SATS Entity Billed (invoiced), Contractor's Invoice reference Number, Invoice Date, Invoiced Currency, Performance/end results required of works done, SATS Equipment ID, Brief description of work scope, Number of man hours charged, Lead time to complete work, Unit of measure for work completed (e.g. Sqm, meters run, Kg, m3 etc.), Unitized Qty of (work) completed (e.g. 12 SqM, 3Kg, 9meters, 6m3 etc.), \$ Rates charged for (any) Ad Hoc Unscheduled works/services/repairs, \$ Regular Fixed Fees charged for regular scheduled works/services (monthly, weekly etc.), Invoiced Total Amount \$ (excluding GST & taxes), Name & email address of the SATS staff (& Department) to whom the invoice is addressed to, (where applicable) Service Report (SR) No, SATS Cost Center (Where known), SATS PO numbers or Award Letter ref. No#, (any) Credit Notes, concessions, discounts etc. (stating the amount), (where applicable) Credit Note Reference Number. And "Issue Log" in a format defined by SATS.

3. Peripherals

3.1 Vendor shall propose the peripherals (e.g. Mobile devices, printer, scanner etc.) which shall not limited to the devices mentioned in the Annex 10

4. User Access Control/Security Requirements for Website Login

- 4.1 The System shall restrict access to the password authentication module to designated administrators of the System only
- 4.2 Corporate Customer user login can be created by SATS super users with compulsory information: Name, Company, email address, validity dates.
- 4.3 Password reset function (for administrator and for user's self-service).
- 4.4 Password must be reset upon first login. This shall be enforced by systems where possible.
- 4.5 Password must be at least 8 characters in length for user account.
- 4.6 Password must be at least 12 characters in length for administrator account.
- 4.7 Password must contain characters from three of the following four categories:
 - 4.7.1 Lowercase characters [a through z]
 - 4.7.2 Uppercase characters [A through Z]
 - 4.7.3 Numbers [0 through 9]
 - 4.7.4 Special characters [e.g. !, @, #, \$, %]
- 4.8 Password must be changed every 90 days or less.
- 4.9 Passwords which have been used for the last 7 changes must not be reused.
- 4.10 Password retries must be restricted to a maximum of 5 attempted logons, after which the user ID must be locked out.

5. Performance

- 5.1 The required end-to-end response time shall be within 3 seconds (Vendor is required to specify their specifications).
- 5.2 Projected no. of concurrent users on average : Around 150
- 5.3 Projected number of concurrent users at peak: Around 200
- 5.4 Vendor shall propose the recommended bandwidth to support the response time as stated in 6.1.
Estimated client bandwidth: Heavy (>20 kbps)

6. Audit Trail Logging

- 6.1 In addition to the Annex 12 Section 7, vendor shall provide below logging capabilities
- 6.2 Login and Logout date/times, User IDs and what screens accessed must be logged for all Users in the audit trails.
- 6.3 All invalid access attempts must also be logged in the audit trails.
- 6.4 All transactions made by the users must be logged with transaction details, date/time and User ID. The auditing and logging shall be operational at all times for all identified transactions that are accounted for in the System

- 6.5 All changes made to the Database, including data creation, data change and data delete must be logged with transaction details, date/time and User ID.
- 6.6 The data within the audit trails must not be removed.
- 6.7 Information shall be displayed in a chronological order.
- 6.8 These audit trails must be available for viewing and printing. Viewing and printing of the audit trails should only be available to the SATS Power User and/or Administrator.
- 6.9 The System shall automatically generate daily and monthly audit reports, including unique cases flagged in audit trail to the SATS Power User and/or Administrator. Vendors shall propose the details required to be listed in the reports in their submission. The details/changes required for these reports shall be finalized during the requirement gathering stage.
- 6.10 All reports shall be exportable for filing purposes. The Vendor shall provide capabilities to generate audit reports in different formats, based on parameters input by the administrator.
- 6.11 The System shall record all activities carried out by privileged accounts including system administrators, auditors, database administrators, network administrators and any other administrator accounts.
- 6.12 Archival and housekeeping script of the logs must be provided. Vendor should ensure that system has enough capacity to hold audit logs for a minimum period of twelve (12) months

7. System Logs

- 7.1 In addition to the Annex 12 Section 7, vendor shall provide below logging capabilities
- 7.2 All system processes and activities must be captured and reviewed periodically. There must be measure to ensure the contents of all logs are not modified and deleted. The log should include a text description of the activity, a date stamp and a time stamp.
- 7.3 All system errors in the application must be logged. The error messages must include a text description of the error, a date stamp and a time stamp.
- 7.4 The System shall automatically generate daily and monthly error logs to be routed to the Power User and/or Administrator in excel file and PDF format. The format and details required for these reports shall be finalized during the requirement gathering stage.
- 7.5 The auditing and logging shall be operational at all times for all identified transactions that are accounted for in the System
- 7.6 The System shall perform the following auditing processes:
 - a) Monitoring of user logins (including successful and unsuccessful attempts);
 - b) Monitoring of access violations from local and remote requests;
 - c) Monitoring of administration tasks performed on the System;
 - d) Monitoring of security profile changes;
 - e) Field validation failure;
 - f) Aggregating errors generated by the System; and
 - g) Notifying the support staff when specific events, such as errors or database failures, are detected.
- 7.7 All reports shall be exportable for filing purposes. The Vendor shall provide capabilities to generate audit reports in different formats, based on parameters input by the administrator.
- 7.8 The System shall record all activities carried out by privileged accounts including system administrators, auditors, database administrators, network administrators and any other administrator accounts.

7.9 Archival and housekeeping script of the logs must be provided. Vendor should ensure that system has enough capacity to hold system logs for a minimum period of twelve (12) months.

8. System Availability (Agreed Service Hours)

8.1 The System shall be fully operational 24 hours a day, 7 days a week (including Public Holidays and Sundays), excluding any planned downtime. Application availability shall be at least 99.5% (i.e. 3.6 hours of unplanned downtime is allowed per month).

9. Error handling

9.1 In addition to the Annex 12 Section 6, vendor shall provide below error handling capabilities

9.2 Errors shall be handled throughout the entire system.

9.3 The system shall:

- a) Display all error responses;
- b) Provide logged errors in a log file.

9.4 Vendor should ensure that system has enough capacity to hold error logs for a minimum period of 90 days.

10. Housekeeping and Archival Requirements

10.1 Transaction data which is older than 12 months shall be archived by housekeeping jobs.

10.2 All data is to be archived for 2 years and shall be stored at a separate server with appropriate dual back-up source.

10.3 Archived data shall be retrievable by SATS Power User and/or Administrator for viewing and investigation purposes.

11. TECHNICAL REQUIREMENTS

11.1 Vendor is required to comply with the following:

- a) Propose specification that meets or exceeds the minimum requirements outlined in Annex 9 (Information Security Requirement).
- b) Specification of the solution for both options shall be equivalent.

11.2 For Cloud hosting - Ensure that the proposed solution is compliant to Annex 10 (Infrastructure & Architecture Standards) and Annex 11 (IT Operations Standards and Guidelines)

11.3 Vendor shall provide the following specification:

- a) Environment (Production, SIT and UAT)
- b) Function (Application/Database)
- c) Operating System
- d) CPU/Core
- e) Quantity
- f) RAM (GB)
- g) SAN (GB)
- h) Sub-System (e.g. MS SQL)

12. USER TRAINING

- 12.1** Vendors shall propose, conduct and implement a training plan to ensure that all SATS trainers and/or testers are competent to perform the necessary testing prior to cutover, and after cutover of the System. This includes the tasks, style of delivery, recommended class size, duration, deliverables and training materials (training guide, user manual and training videos for all features for all key user roles) needed for the training plan. The System shall be designed intuitively, easy for staff to understand and navigate and not require extensive training.
- 12.2** Vendor shall provide minimally separate training session before beginning of UAT testing and before commissioning of system.

13. TESTING & ACCEPTANCE

- 13.1** The appointed Vendor shall:
- a) Work with all relevant 3rd party vendors 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) Prepare test data;
 - d) Conduct functional testing, unit testing, system integration testing, user acceptance testing and performance testing;
- 13.2** All tests shall be conducted in the presence of appointed representative from SATS to the satisfaction of SATS. The Vendor shall supply all necessary testing software tools, connections and skilled labor required for the tests to be carried out to the satisfaction of SATS, without separate charges to SATS.
- 13.3** Acceptance of the service/hardware will be based on the 100% compliance to configuration requirements within the scope.
- 13.4 System Integration Testing (SIT)**
- 13.4.1** SIT which requires integration with other SATS internal/external system will be conducted jointly with SATS Technology representatives.
- 13.4.2** Integration test within system will be conducted by Vendor before ready for UAT.
- 13.4.3** Vendor shall adhere to strict application and software code version control protocol.
- 13.4.4** The System is considered ready for UAT only if SIT meets the following:
- a) Successful execution of the test scripts (i.e. 100%);
 - b) Functional, Performance and Availability Requirements are met;
 - c) There is zero defects of Severity 2 and Severity 3 problems (refer Annex 8.1, 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).
- 13.5 User Acceptance Testing (UAT)**
- 13.5.1** The System will be accepted and released for Production only if UAT meets the following:
- i. Successful execution of the test scripts (i.e. 100%);
 - ii. Functional, Performance & Availability Requirements are met;

- iii. There is zero defects of Severity 2 and Severity 3 problems (refer Annex 8.1, section 4.2, for SLA definition); and
- iv. 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 production move.

13.5.2 In the event when the number of defects in UAT exceeds 0.25 of the Defect Density (Defect Density = Number of Defects / Total Number of test Cases), SATS has the right to call off the UAT and request the appointed Vendor to re-do Unit Testing and SIT and rectify all defects before UAT is re-initiated. All such retesting shall be conducted by the appointed Vendor at no additional cost to SATS.

13.5.3 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 8.1, Section 4.4) in the event the outstanding Severity 4 issues are not resolved.

13.5.4 Vendor shall adhere to strict application and software code version control protocol.

14. WARRANTY PERIOD

14.1 Vendors shall quote for :

- One (1) month warranty period, and
- Three (3) months warranty period.

The final Warranty Period shall be decided by SATS, at its sole discretion.

14.2 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 8.1, Section 4.4) in the event the outstanding Severity 4 issues are not resolved.
- c) Maintain the list of post-cutover 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.
- h) Troubleshoot interface problems with 3rd party interfacing systems and ensure problems are resolved.
- i) 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.

14.3 The appointed Vendor shall define clearly the proposal support structure to support the Warranty Period.

14.4 The appointed Vendor shall provide resources and workflows in place to accept and manage incidents.

14.5 The Incident Management processes are shown in Annex 8.2 (Service Level Agreement – Incident Management)

14.6 The support provided by the appointed Vendor during the Warranty Period shall adhere to the Service Level Agreement (SLA) as stipulated in Annex 8.1 (Service Level Agreement during Warranty Period)

14.7 The warranty period shall commence only after the official sign off from SATS has been completed (UAT sign-off conditions mentioned in Section 14.5 must be met). Successful completion of the Warranty Period

is subject to the fulfillment of the requirements stipulated in Section 14.5.2 and upon official sign-off from SATS. Do note that 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 cost to SATS.

15. APPLICATION MAINTENANCE

- 15.1** The vendor shall propose the following two (2) options:
- a) Option A - Provide Sev 2 (High) maintenance support.
 - b) Option B - Provide Sev 3 (Medium) maintenance support.
- 15.2** The appointed Vendor shall comply with the requirements under Annex13 (Application Maintenance Services)
- 15.3** The Vendor shall incorporate an agreed number of man-hours in the annual maintenance contract (at no extra charge) for billing configuration works (for new customers) and to quote for man-hour rate if the efforts to configure new requirements exceeds the declared man-hours under the annual maintenance contract.
- 15.4** All upgrades due to programming bugs shall be provided free of charge by the Vendor.
- 15.5** The Vendor shall work with SATS to conduct the following activities where applicable:
- a) Network vulnerability scanning
 - b) Host based vulnerability scanning
 - c) Web application vulnerability scanning
 - d) Penetration testing
 - e) Source Code Review/Scanning
- 15.6** SATS reserves the rights to engage the service of an independent consultant to conduct similar security and vulnerability test on System on periodic basis (e.g. once every three (3) months). The Vendor shall provide necessary support, including reports to the independent consultant for the conduct of the security and vulnerability at no additional cost to SATS. The security and vulnerability test done by SATS appointed independent consultant includes the following:
- a. Authentication testing,
 - b. Security Perimeter testing,
 - c. Web Application testing,
 - d. Session handling testing,
 - e. Error handling testing,
 - f. Access Control and Authorization testing,
 - g. Unauthorized Data Alteration and Disclosure testing, and
 - h. Code review on the security risks and performances issues identified from test findings.
- 15.7** If any security weaknesses and performance issues have been found on the system, the Vendor shall, at no additional cost to SATS, implement the necessary security controls and countermeasures as recommended by the independent security consultant in order to eliminate/minimize the security risks and performance issues
- 15.8** If the security and vulnerability test is conducted after system commissioning, the Contractor shall implement the test findings and recommendations no later than <one (1) month> upon notification by

SATS. The timeline for mitigating the identified vulnerabilities shall be based on the level of criticality and agreed SLA

- 15.9** The Vendor shall disable remote administrative access to their servers if they do not need this functionality. If remote administrative access is required, the Vendor shall put in place all of the following security measures:
- a. Remote administrative access shall only be granted to authorize personnel who need to administer their servers remotely;
 - b. Remote administrative access shall only be done by authorized personnel from specific systems and filtering based on IP address shall be implemented;
 - c. Personnel that are authorized to have remote administrative access shall use 2-factor authentication to authenticate to the servers; and
 - d. Logging of the Date and Time, IP addresses of the source and destination systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access.
- 15.10** Vendor shall adhere to strict application and software code version control protocol.

16. INFRASTRUCTURE REQUIREMENTS

16.1 Vendors shall provide the infrastructure diagram and hardware specifications required from SATS for the smooth running of the application.

Please indicate:

Operating Server required

Number of CPUs/Cores required per Server

RAM (GB) required per Server

Storage (GB) required per Server

Database software required

Other Software required

16.2 Vendors shall quote for below:

Cloud-hosted: Using external cloud hosting solution MS Azure

16.3 Vendors shall provide the servers specification (e.g. hardware sizing) and licenses Requirements.

16.4 Vendor shall also quote and include the specification details on the Managed Hosting Services as specified in the section 16.5

16.5 Scope of Work for Managed Cloud Services

16.5.1 The Vendor shall provide incident, problem and change management including:

- a. Log and report collection
- b. Cause analysis
- c. Troubleshooting
- d. Workaround deployment
- e. Fix deployment
- f. Testing
- g. Performance Management
- h. Asset Management, create and maintain a document of record to all assets and key configurations

16.5.2 The Vendor shall provide support to VMs including:

- a. VM updating, upgrading and patching
- b. VM hardening and policy enforcement
- c. VM performance monitoring and optimization
- d. VM system administration and troubleshooting
- e. VM software distribution
- f. VM task scheduling for automating repeated activities with scripting
- g. VM syslog management and review

16.5.3 The Vendor shall provide support to Storage including:

- a. Storage mapping to VMs
- b. Storage backup and restore maintenance
- c. Storage policy maintenance like retention period
- d. Monitor and manage storage
- e. Perform periodic checks and ensure the integrity of backups

16.5.4 The Vendor shall provide support to Cloud Hosting Load Balancer and Network including:

- a. Maintain and manage networks such as Virtual Networks, and Subnets
- b. Maintain and manage access control with Network Security Groups, NACL and routing tables
- c. Maintain and manage load balancer configurations
- d. Monitor network access

16.5.5 The Vendor shall provide support on backup, recovery, and disaster recovery for cloud hosted services including:

- a. Recovery assurance for daily operational services
- b. Periodic reporting for any emergency arising from cloud provider infrastructure services

16.5.6 The Vendor shall provide support to Database including:

- a. Database services monitoring
- b. Database backup and restore

16.5.7 The Vendor shall provide Cloud Hosting Services Management including:

- a. Cloud hosting change management
- b. Cloud hosting reporting management
- c. Cloud hosting service account management
- d. Cloud hosting usage and billing management

16.5.8 The Vendor shall provide Security, Process and Compliance Management including:

- a. Information Security baseline review
- b. Identity and Access Management:
 - i. Creating;
 - ii. Distributing;
 - iii. Rotating;
 - iv. And revoking user accounts
- c. Security Scanning and Patching
- d. Process Implementation and Management aligning to ISO 20000-1:2011 (ITSM)
- e. Process Implementation and Management aligning to ISO 27001:2013 (ISMS)

17. PROJECT MANAGEMENT

- 17.1** 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 interface developments, testing and implementation (where needed by SATS).
- 17.2** 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 SATS overall Project Manager & SATS Technology Project Manager to manage and drive the end-to-end delivery of the project;
 - b) Work with SATS' Technical Services and Operation (TSO) 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 schedules;
 - f) Provide regular updates on the progress of the project;
 - g) Comply with industry practices and standards for project management and infrastructure design.
- 17.3** 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' prime and single point of contact.
- 17.4** All Vendors shall furnish the project organization structure, escalation process and resumes of ALL key members (inclusive of the propose Project Manager). SATS reserves the right to request for a change of resources.
- 17.5** Project Schedule
- 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 testing, SIT, UAT schedules;
 - c. Training schedules, including User training before and after UAT and before cutover;
 - d. Preparatory work prior to UAT and cutover;
 - e. Resolution of defects found during UAT
 - f. Development, testing and implementing of all interface systems and/or external systems and/or parties;
 - g. Support during cutover, and Warranty Period
- 17.6** Project Deliverables
- As part of the implementation, the following project documentations shall be delivered during the Project Life Cycle (including but not limited to):
- 17.7** Planning Phase
- a) Project organization structure, with defined roles and responsibilities
 - b) 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
 - c) Project kick-off deck

17.7.1 Design Phase

- a) Overall and detailed system design document and Sign-off
- b) System Architecture and design
- c) System Account roles and responsibilities
- d) System Security Configuration
- e) Functional Specifications and Sign-off.

The document should consist of:

- i. FHD (Functional Hierarchy Diagram to show relationship and hierarchy of modules) or Use Case Model Survey
 - ii. Data Model (e.g. ERD – entity relationship data)
 - iii. High level workflow/process flow description, if any (e.g. flowchart or activity diagram)
 - iv. Interfaces to existing and/or new systems (include description of these systems (functional and technical platform), data, interface method, frequency, availability, a detailed diagram depicting the interfaces, etc.)
- f) Prototype screens and Sign-off
 - g) Database schema and Sign-off
 - h) Test plan and Sign-off

17.7.2 Development Phase

- a) Test Plan, scenarios, test scripts, results and acceptance criteria (covering Functional, Integration and Performance testing) and Sign-off
- b) Training plan (includes TTT – train the trainer) and Sign-off
- c) Training schedule and materials (both hardcopy and softcopy) and Sign-off
- d) User Guide/manual and Sign-off
- e) SIT Report

17.7.3 Deployment Phase

- a) System Administration Guide and Sign-off
- b) Application maintenance Guide and Sign-off
- c) Installation and Configuration Guide and Sign-off
- d) Program Loading Guide and Sign-off
- e) Updated Integration/technical landscape and Sign-off
- f) Implementation Plan, Checklist and Sign-off
- g) Post Implementation Support Plan and Sign-off
- h) Certified Audit Report (proof of compliance with SATS Information security policy, information security standard, IT security framework, Implementation standards, technical standards and procedures)
- i) Review and Rectify findings from Penetration Test Report

17.7.4 Post-Production and Monitoring Phase

- a) List of outstanding system issues/defects, impact analysis and severity categorization
- b) Updated Change request Log with detailed requirements, man-effort sizing and Sign-off
- c) Post Implementation review report and Sign-off

17.7.5 For All Phases

- a) Weekly Project Status Report
- b) Project Risk and Mitigation Plan

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

ANNEX 15: PRICING TABLE

S/N	Description	Pricing (SGD)		
		Quantity	Unit	Total
1	Software and Licenses (SAAS)			
2	<p>Video Analytics (per use-case basis)*</p> <p>a) Verification of harness was donned during the aircraft cabin door opening and closing</p> <p>b) Verification of lifeline attachment onto the harness worn by staff during the aircraft cabin door opening and closing</p> <p>c) Verification of double stacking of containers and items on meal carts</p> <p>d) Verification of Hi-Lift Platform Hand Rails deployment during cabin loading and unloading process</p> <p>e) Verification of correct marshalling technique used by marshaller during marshalling of Hi-Lift in docking operations</p> <p>f) Verification of circle of safety checks during Hi-Lift docking operations</p> <p>g) Verification of Frisking of Door during aircraft cabin door closing</p> <p>h) Self-diagnosis of Hi-Lift CCTV tampering</p> <p><i>*SATS will make payment for individual use-case if a minimum accuracy of 80% is achieved</i></p>			
3	<p>One-Time Implementation Cost (please itemize)</p> <p>a) Project Management</p> <p>b) Requirements and Design</p> <p>c) Build and Test</p> <p>d) Cutover</p>			
4	<p>Hardware Cost (please itemize)</p> <p>a) Servers</p> <p>b) NVR / DVR / Edge Devices</p> <p>c) Cameras</p> <p>d) Monitors / Tables</p> <p>e) Cabling</p>			
5	Option A: One (1) month warranty			
	Option B: Three (3) months warranty			
6	<p>Training</p> <p>- State how many days of training quoted</p> <p>- Quote for per man-day training rate if additional training is required</p>			
7	<p><u>Option A:</u> Provide 24 hours x 7 days maintenance support and helpdesk hours for Sev 2 (High) maintenance support</p> <p>Maintenance and Support Services (after warranty)</p> <p>a) 1st year</p> <p>b) 2nd year(optional)</p> <p>c) 3rd year(optional)</p> <p>d) 4th year (optional)</p> <p>e) 5th year (optional)</p>			

	Option B: Provide 24 hours x 7 days maintenance support and helpdesk hours for Sev 3 (Medium) maintenance support Maintenance and Support Services (after warranty) a) 1st year b) 2nd year(optional) c) 3rd year(optional) d) 4th year (optional) e) 5th year (optional)			
8	Manage Cloud Services (for Cloud hosted) (Optional) a) 1st year b) 2nd year(optional) c) 3rd year(optional) d) 4th year (optional) e) 5th year (optional)			
9	Man-day rate			
10	Man-month rate			
11	Other expenses (if any)			

Vendors to provide all details pertaining to the pricing for the submitted proposal, the validity shall be for a period of Twelve (12) 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 15: 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):

Upon verification of successful identification of the use case <i>(value determined by the number of successful use cases out of 8)</i>	10% of Tender Amount
Upon acceptance of System Integration Tests (SIT)	10% of Tender Amount
Upon acceptance of User Acceptance Tests (UAT)	15% of Tender Amount
Upon Implementation in 02 HL with live system	15% of Tender Amount
Upon Implementation in 10 HL with live system	10% of Tender Amount
Upon Implementation in 20 HL with live system	10% of Tender Amount
Upon Implementation in 35 HL with live system	10% of Tender Amount
Upon end of Warranty Period	20% of Tender 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 16: IMPLEMENTATION CONTRACT

<<< [Implementation 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 Implementation Contract	Compliance	Remarks
1	Definitions and Interpretation		
1.1	In this Agreement, unless the context otherwise requires: Acceptance Date means the date on which SATS accepts the System in accordance with Clause 6.4	Y	

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

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

Figure 3: Sample of Compliance Table for Annex 16

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

APPENDIX A (1): ENVELOPE LABEL FOR TENDER SUBMISSION

Envelope Label:

Tender No: CT2103J003
Tender Closing Date and Time: **14-MAY-2021** – 12 NOON, SINGAPORE TIME
Tender Description: TENDER FOR **Outdoor Hi-Lifts Video Analytics (VA) Phase 2**
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 IN-FLIGHT CATERING CENTRE 1
20 AIRPORT BOULEVARD
SINGAPORE 819659**

FROM:

Name of Business Firm/Company:
Address:
Telephone and Fax Number:
Contact Person(s):