

PART 2

REQUIREMENTS SPECIFICATION

TABLE OF CONTENTS

1.	INTRODUCTION.....	ERROR! BOOKMARK NOT DEFINED.
1.1.	Overview	6
1.2.	Background	6
1.3.	Key Objectives	6
2.	SCOPE OF TENDER	8
2.1.	General	8
3.	FUNCTIONAL REQUIREMENTS	10
3.1.	Overview	10
3.2.	Detailed Functional Requirements	11
4.	DATA CONVERSION AND MIGRATION	12
4.1.	Overview	12
5.	SYSTEM PERFORMANCE, AVAILABILITY AND RELIABILITY	16
5.1.	System Load	16
5.2.	System Scalability	16
5.3.	System Reliability	16
5.4.	System Availability	17
5.5.	System Performance Test Parameters and Exit Criteria	18
6.	SYSTEM MAINTENANCE AND SUPPORT SERVICES	22
6.1.	Overview	22
6.2.	Full Maintenance Support	22
6.3.	Ad-Hoc Support	25
6.4.	Database Administration and Support	25
6.5.	System Maintenance and Support Plan	28
6.6.	Middleware Administration and Support	29
6.7.	Second Level Helpdesk	Error! Bookmark not defined.
6.8.	Standards and Procedure	31
6.9.	Maintenance Log	31
7.	SUPPORT HOURS AND OPERATING HOURS	32
7.1.	Overview	32
8.	SERVICE REQUESTS	33
8.1.	Overview	33
8.2.	Service Request Procedure	35
8.3.	Service Request Service Levels	36
8.4.	Turnaround Time	37
9.	PROBLEM ESCALATION, ANALYSIS, RESOLUTION AND MANAGEMENT	38

9.1.	Problem Management	38
10.	TECHNICAL REQUIREMENTS.....	45
10.1.	General Requirements	45
10.2.	System Environment	45
10.3.	Data Backup & Restoration	46
10.4.	Development Facility Requirements	47
10.5.	System Architecture	48
10.6.	Technical Design Consideration	48
10.7.	Interface Requirements	50
11.	INTENTIONALLY LEFT BLANK	52
12.	SECURITY REQUIREMENTS	53
12.1.	General Security Requirements	53
12.2.	Assets Management	54
12.3.	Information Classification and Handling	54
12.4.	Personnel Requirements.....	56
12.5.	Security Risk Management	56
12.6.	Security Monitoring	58
12.7.	Security Testing	58
12.8.	ICT and Data Security Incident Management.....	61
12.9.	Security Training and Awareness	63
12.10.	Business Continuity Management	64
12.11.	System Security.....	64
12.12.	Network Security	68
12.13.	Application Security	71
12.14.	Access Control	74
12.15.	Data Confidentiality and Integrity	78
12.16.	Personal Data	79
12.17.	Cryptography	82
12.18.	Information Backup Security	85
12.19.	Change Management and Patch Management	85
12.20.	Vulnerability Management	87
12.21.	Systems using Commercial Cloud	88
12.22.	Logging and Audit Trails	89
13.	TESTING, SYSTEM DELIVERY AND ACCEPTANCE REQUIREMENTS ..	92
13.1.	General Requirements.....	92
13.2.	Test Levels and Test Types.....	94
13.3.	Test Level: Unit Testing	96

13.4.	Test Level: System Integration Testing (SIT).....	97
13.5.	Test Level: User Acceptance Testing (UAT)	98
13.6.	Test Type: Unit Tests	101
13.7.	Test Type: Source Code Review	102
13.8.	Test Type: Compliance Test	105
13.9.	Test Type: Usability Test	105
13.10.	Test Type: Functional Tests	106
13.11.	Test Type: Data Conversion & Migration Test	107
13.12.	Test Type: Integration Tests	107
13.13.	Test Type: Performance Test	110
13.14.	Test Type: Operational Readiness Test	114
14.	PROJECT MANAGEMENT AND QUALITY ASSURANCE	116
14.1.	Project Organisation.....	116
14.2.	Role of Contractor's Project Manager	117
14.3.	Project Management Plan	119
14.4.	Role of the Representative of the School.....	120
14.5.	Progress Reporting.....	120
14.6.	Mobilisation / Replacement of Key Personnel	121
14.7.	Quality Assurance	123
14.8.	Performance Indicator.....	123
15.	COMPLIANCE TO STANDARDS AND METHODOLOGY	124
15.1.	Quality Management System (QMS).....	124
16.	TRAINING	128
16.1.	Overview.....	128
16.2.	General Requirements.....	128
16.3.	Specific Requirements	128
16.4.	Feedback and Evaluation	130
16.5.	Schedule	130
17.	DOCUMENTATION.....	131
17.1.	Overview.....	131
17.2.	General Requirements.....	131
17.3.	Specific Requirements	132
17.4.	Rights to Application and Documentation.....	134
18.	TRANSITION MANAGEMENT	136
18.1.	Overview.....	136
18.2.	General Requirements.....	136
18.3.	Phase-in Transition	136

18.4.	Phase-out Transition	137
18.5.	Exit Plan.....	138

1. INTRODUCTION

1.1. Overview

- 1.1.1. Tenderers are invited to submit a complete proposal for the design, development, delivery, installation, testing, commissioning and maintenance of the integrated Software-as-a-Service (SaaS) solution for Finance, Human Resource and Procurement functions (the “System”) for Singapore Sports School Ltd (the “SSP” or the “School”).
- 1.1.2. The Tenderer shall propose a SaaS solution that meets the requirements of the System. The Tenderer shall configure the SaaS to meet the functional requirements, where possible, Conditions of Contract in Part 1 Section B and shall be applicable to the SaaS and its related works such as, but not limited to, configurations and installations. Functionalities provided by the SaaS or configured in the SaaS shall be developed accordance to functional requirements, and Conditions of Contract in Part 1 Section B.

1.2. Background

- 1.2.1. The School is expanding its business capabilities to better integrate all policies and programme in high performance sports and consolidate all sports science capabilities.
- 1.2.2. This expansion requires an integrated SaaS system to streamline and enhance the efficiency of the financial, human resource, and procurement operations.

1.3. Key Objectives

1.3.1. Improve operational and process efficiency

The integrated SaaS system will leverage existing cloud services to transform corporate services and achieve operational efficiency on an integrated SaaS solution. The System will maintain seamless data integration across Human Resource, Finance and Procurement functions, facilitating a single source of truth and data accuracy throughout all business processes. It will benchmark HR, Finance and Procurement processes to the industry’s best practices to improve process efficiency. The System will also minimise manual processes during data processing to ensure timely financial closing and accurate reporting of financial performance.

1.3.2. Provide centralized visibility

The integrated SaaS system will allow automatic retrieval of, and real-time access to data by management and business units. This will provide real-time data and analytics, enabling managers to make informed decisions about resource allocation and managing shortages or surpluses.

1.3.3. Ensure scalability and flexibility

The integrated SaaS system will be scalable and flexible enough to handle growth, changes in resource demand, or shifts in organisational structure and strategy. It will also provide for the necessary interfaces with external systems for data integration and consolidation.

1.3.4. Support compliance and risk management

The integrated SaaS system will leverage system functionalities to perform control checks so as to ensure compliance to applicable policies and processes, and relevant laws and regulations.

1.3.5. Cost efficient delivery of HR, Finance and Procurement services

The integrated SaaS system will deliver HR, Finance and Procurement services in a cost-efficient manner to achieve expected cost savings from adopting SaaS.

2. SCOPE OF TENDER

2.1. General

2.1.1. The Tenderer shall submit the proposal in accordance with Part 2 Requirement Specifications as stipulated in this Tender.

2.1.2. The Tenderer shall propose and quote separately for the Base and Optional Services and items. The School reserves the right to award any Optional Services or Items at its sole discretion at time during the Contract period. The scope of tender shall be as follows:

Base Services

- (a) Supply, delivery, design, develop, install, test, migrate existing data and commission a complete suite of the System within Implementation Period of **NINE (9) months** from the contract start date for Phase 1 and **NINE (9) months** for Phase 2, unless otherwise specified or agreed by the School in writing.
- (b) Provide for necessary interfaces between the System and other systems within and outside the School (the “External Systems”) for data integration and consolidation.
- (c) Provision of software license for SaaS system for a period of **THREE (3) years.**
- (d) Provide Sixty (60) calendar days Performance Guarantee Period (PGP).
- (e) Provide the Application Software Maintenance and Support services, including day to day application support, to take effect upon expiry of the PGP, for a period of TWO (2) years.

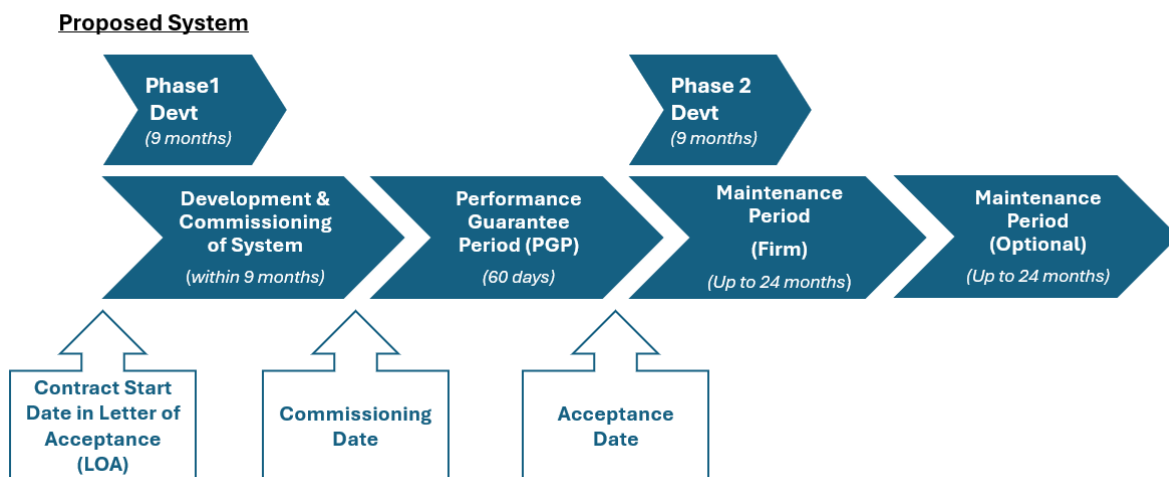
Optional Services and Items

The School may, at its own discretion, require the Contractor to provide the following optional services and items:

- (f) Provide the Application Software Maintenance and Support services for the System following the expiration of services required in **Clause 2.1.2e**, for a period of **TWO (2) years,** to be exercised by the School.
 - (g) Provision of software license for SaaS system for a period of **TWO (2) years.**
- 2.1.3. Any other items necessary for the working of the System not clearly indicated by the Tenderer shall be deemed to be an intrinsic part of the System and their cost, if any, shall be included as part of the System.

- 2.1.4. The System shall be designed to support the following indicative user base of the School:
- (a) Total employee population: Approximately 500 users.
 - (b) Core Corporate Services function users:
 - (i) Human Resources: Approximately 8 officers;
 - (ii) Finance: Approximately 10 officers; and
 - (iii) Procurement: Approximately 7 officers.
- 2.1.5. The Contract shall commence on the contract start date stated in the Letter of Acceptance (LOA).
- 2.1.6. The timeline for this Contract is illustrated as follows and time shall be of essence for the Contractor in meeting the said timeline, unless otherwise specified or agreed by the School in writing:

Figure 1: Timeline



3. FUNCTIONAL REQUIREMENTS

3.1. Overview

- 3.1.1. The following depicts the planned modules for Phase I and II of the development phase. Unless otherwise specified by the School in writing, these modules/functions shall be implemented according to their respective phases as outlined below:

	Phase I (Essential Modules/Functions)	Phase II (Secondary Modules/Functions)
Finance	<ul style="list-style-type: none"> a) Budgetary Control b) Fixed Asset Management c) Account Receivables d) Staff Claims e) Account Payables f) Cash Management g) General Ledger h) Projects 	
Human Resource	<ul style="list-style-type: none"> a) Organisation Management b) Worker Profile c) Compensation d) Leave Administration e) Employee Benefits Administration f) Payroll i) Employee Self-service 	<ul style="list-style-type: none"> a) Recruitment b) Learning & Development c) Performance Management d) Workforce Lifecycle Management e) Attendance/Time Administration
Procurement	<ul style="list-style-type: none"> a) Approval of Requirements b) Small Value Purchase c) Sourcing d) Evaluation and Approval Contracting e) Contract Management f) Revenue Contracting 	
General System Features (common across all functions)	<ul style="list-style-type: none"> a) User Account Management b) Workflow Management c) Document Management d) Basic Reporting e) Integration Capabilities f) Mobile Accessibility g) Collaboration Features h) System Administration 	<ul style="list-style-type: none"> a) Advanced Data Analytics b) Automation Tools

3.2. Detailed Functional Requirements

Clause	Functional Area	Detailed Specifications
3.2.2a	General System Features Requirements - Firm	Please refer to Annex A - <u>General</u> worksheet for the detailed specifications.
3.2.2b	General System Features Requirements – Optional	
3.2.2c	Finance Functional Requirements - Firm	Please refer to Annex A - <u>Finance</u> worksheet for the detailed specifications.
3.2.2d	Finance Functional Requirements – Optional	
3.2.2e	Human Resource Functional Requirements - Firm	Please refer to Annex A - <u>Human Resource</u> worksheet for the detailed specifications.
3.2.2f	Human Resource Functional Requirements – Optional	
3.2.2g	Procurement Functional Requirements - Firm	Please refer to Annex A - <u>Procurement</u> worksheet for the detailed specifications.
3.2.2h	Procurement Functional Requirements – Optional	

4. DATA CONVERSION AND MIGRATION

4.1. Overview

- 4.1.1. The Contractor shall carry out conversion and migration of all data (include historical data) to the proposed database system in the configuration, User Acceptance Test (UAT) and production environments of the System without any data loss or distortion, from the existing system.
- 4.1.2. The Contractor shall study in greater details during the requirement study to securely migrate the data from these databases to the System.
- 4.1.3. The Contractor shall analyse users' requirements and propose a detailed Data Conversion and Migration Plan for the School's approval. The Data Conversion and Migration Plan shall include, at minimum, submissions in the following areas:
- (a) Securing the data at rest and in motion during data conversion and migration.
 - (b) Data conversion strategy, approach, the estimated duration and activities related to conversion of existing data to the new format in the System.
 - (c) Migration strategy, approach and activities related to trial and actual migration of existing data to the new environment, such as data mapping, cleaning, and data conversion;
 - (d) Specify clearly the critical path and the critical success factors;
 - (e) Verification to ensure data integrity and completeness;
 - (f) Exception and error-handling process; and
 - (g) Contingency plan for failed data migration process.
- 4.1.4. Where the activities require user involvement, the Contractor shall automate as far as possible all the preparation of the data prior to user involvement. Such activities shall include the following:
- (a) Seek confirmation from the users on the data items to be converted and migrated as well as any uncertainty encountered during the conversion of data;
 - (b) Perform data item validation, compatibility checks between data items and checking for duplicates in the current system;
 - (c) Coordinate data correction and data collection;
 - (i) Provide batch facilities to update correction of data and insert missing data. This shall be the modus operandi for the data cleaning

- activities;
 - (ii) Manage the entire process for data conversion and migration; and
 - (iii) Verify the new databases created and reconciliation of the number of records created between the existing system and new system.
- (d) The Contractor shall submit the following documents to the School for review and approval during the data conversion and migration process:
- (i) Conversion and Migration Specifications, outlining the mapping of data fields from original format to the new format required;
 - (ii) Conversion and Migration Test Plan;
 - (iii) Conversion and Migration Test Scenario and Results; and
 - (iv) Conversion and Migration Test Report.
- (e) The Contractor shall perform all data conversion where necessary or where required by the School. The details of the conversion shall be stated clearly in the Data Conversion and Migration Plan.
- (f) The Contractor shall develop a data cleansing strategy to ensure data consistency and quality. The Contractor shall assist the School's users to conduct data cleansing prior and throughout the data migration exercise or when requested by the School.
- (g) The existing vendors of the System to be migrated shall only be providing the source data for migration in exported .csv or equivalent formats. Upon receipt of such data from the existing vendors, the Contractor shall perform all data mapping and conversion activities required to complete the migration based on the School's requirements.
- (h) The Contractor shall only be granted restricted access to the existing systems' databases only from pre-identified network addresses. The School reserves the right to grant limited access to the existing systems' data according to the migration plan.
- (i) The Contractor shall propose a validation and verification methodology and perform all necessary tests to ensure the accuracy and completeness of the migrated data and security/access control information.
- (j) The data migration shall be carried out, with minimal downtime and disruption to the business operation. The School may occasionally request the Contractor to carry out data conversion/migration work after office hours. All other additional expenses incurred for after-office hours work shall be borne by the Contractor.
- (k) The Contractor shall ensure that data conversion / migration shall not affect the existing systems' daily operations and that minimal effort is required by the users for the conversion / migration process.

- (l) The Contractor shall take all necessary precautionary measures to ensure their migration strategy shall not incur any risk to the production server. The Contractor shall test the migration procedures and conversion programs thoroughly before commencing the migration process.
- (m) The Contractor shall ensure that the migration and conversion programs, the data migrated and converted are free of errors. The Contractor shall rectify any errors detected at no cost to the School.
- (n) The Contractor shall also be responsible to liaise with any relevant parties, including existing maintenance vendors, at no cost to the School.

4.1.5. The list of datasets to be migrated to the System include the following:

Functional Area	Details of dataset	Minimal Data	Additional Data
Finance	General Ledger Comparative balances	5 years	Previous 2 years
	Master data (customers and Contractors)	Full set	N.A
	Assets (fixed assets and low value assets)	Full set	
HR	Active Employee	Full set including history Exclude inflight job requisition, historical supervisory org hierarchy	N.A
	Inactive Employee in current year	Full set including history	N.A
	Inactive Employee	Basic	N.A

	in previous years	personal data and blacklist information	
Payroll	Active Employee	Full payroll result including current and previous year (Jan to Dec)	N.A
	Inactive Employee	Full payroll result including current and previous year (Jan to Dec)	N.A
Procurement	Information on Existing Contracts	Full set of contract details	N.A
	Open items (include, but not limited to, Purchase Requisitions, Purchase Orders, customer invoices, Contractor invoices, contracts, Work in Progress (WIP) items)	Full set	N.A

5. SYSTEM PERFORMANCE, AVAILABILITY AND RELIABILITY

5.1. System Load

- 5.1.1. The System shall support One Hundred (100) concurrent users across all modules in the System.
- 5.1.2. As a guide, the projected growth of concurrent user base shall be based on 5% of the present concurrent user base per annum for up to FOUR (4) years from the Acceptance Date.
- 5.1.3. The Tenderer shall provide detailed information/algorithm to demonstrate how the system capacity sizing is derived in their tender proposal.

5.2. System Scalability

- 5.2.1. High system scalability is an important requirement for the System to be developed. The System shall be able to scale up to meet the growth in data load and the numbers of users through straight-forward upgrade of system software/hardware components (with probably additional software licences) without having to compromise on the system performance or changing the design/architecture set up of the System.
- 5.2.2. The proposed hardware and peripherals (if applicable) MUST be scalable to support the increase in application and system load. The Contractor shall be responsible for replacing the System and peripherals at no additional cost to the School if the Contractor is unable to meet the requirement.

5.3. System Reliability

- 5.3.1. The Contractor shall propose automatic recovery and restart procedures/facilities to ensure minimum downtime of the System. The Contractor shall provide clear instructions on such facilities in the tender proposal.
- 5.3.2. Hardware fault in any of the peripherals and/or a software fault in a sub-system shall not lead to total system failure.
- 5.3.3. All software/hardware shall be fully tested prior to implementation in order to ensure a maximum level of reliability of the components. It is the Contractor's responsibility to ensure that the proposal meets the requirement.
- 5.3.4. All the data in the System shall be recoverable to the last successfully completed transaction in the event of failure of the System. Comprehensive logging shall be enabled to facilitate recovery of data for the System and across other systems that have interface(s) to the System.

- 5.3.5. The Contractor shall ensure that all software errors in the System shall not lead to total system failure. The System shall be maintained to handle contention and lock handling between databases and between database tables.
- 5.3.6. The Contractor shall ensure that any failure of any transaction shall not affect integrity of the data captured /stored in the System.
- 5.3.7. The System shall be able to automatically recover all data stored up to the last successfully completed transaction before a system failure occurs.
- 5.3.8. The Contractor shall ensure that all Software and application enhancements or upgrades are fully tested and quality assured prior to implementation in order to ensure a maximum level of reliability of the Software.
- 5.3.9. The Contractor shall perform impact analysis based on the regular patches (for O/S, middleware, etc) to ensure that the application still works. If application changes are required to make it work in the new environment, the Contractor shall provide it as part of the base service.
- 5.3.10. The System shall include online performance monitoring and error analysis reporting to enable proper capacity planning, tuning and maintenance. The Contractor shall provide clear illustrations of such monitoring and reporting facilities in the tender proposal.
- 5.3.11. The System shall provide an effective and automatic unattended backup system.
- 5.3.12. The Contractor shall ensure that there is no loss or distortion of data, interference with system functions, display of erratic information, etc, due to improper operation by maintenance personnel.
- 5.3.13. In the event of power failure, no loss or distortion of data shall occur. The System shall automatically restart and continue operation. In the event of power failure, no loss or distortion of data shall occur. The System shall automatically restart and continue operation. All instances of system downtime shall be recorded with a detailed explanation of the cause and reason for the downtime, and the course of action taken for system rectification.
- 5.4. System Availability**
- 5.4.1. The System shall be required to run continuously for 24 hours a day, 7 days a week, including Saturdays, Sundays and Public Holidays. The System Availability level shall not be less than **NINETY-NINE POINT FIVE percent (99.5%) for each calendar month** or part thereof commencing upon the successful completion of the Performance Guarantee Period (“**Monthly System Availability Level**”). The Contractor shall maintain System Availability and minimise System Downtime.
- 5.4.2. The System shall operate in an unattended mode outside the Operating Hours specified. This period shall be the designated batch window.

- 5.4.3. System Availability is defined as the percentage of the total time during which the System is available to the School and its users. It is calculated as:

$$\text{System Availability} = \frac{SOT - SD}{SOT} \times 100\%$$

where:

SOT: Scheduled Operation Time is defined to be the scheduled operating hours for the System.

SD: System Downtime is the accumulated time during which the System or its component is inoperable or partially inoperable due to system failure.

- 5.4.4. The Contractor shall size and provide a complete system configuration to meet the response time and performance requirements as specified.
- 5.4.5. The Contractor shall also take into consideration audit trail, transaction log, housekeeping and archival requirements when sizing the System.
- 5.4.6. The Contractor shall take into consideration the projected annual growth rate of the System in its planning to meet the required System Availability.
- 5.4.7. The Contractor shall propose resource monitoring to facilitate capacity planning, maintenance and tuning. The Contractor shall provide clear illustrations on such monitoring facilities.
- 5.4.8. The System shall be considered to be inoperable or partially inoperable if any one of the following conditions is met:
- (a) Any of the Proposed System servers becomes inaccessible;
 - (b) Any of the crucial services on any of the System servers becomes inaccessible (e.g. Database service becomes inaccessible on the System Production Environment);
 - (c) Any of the crucial services on any of the System servers does not respond properly (e.g. Loss of data from remote sensors); or
 - (d) Any of the crucial business applications on any of the System servers becomes inaccessible (e.g. Administration module becomes inaccessible on the System Production Server).

5.5. System Performance Test Parameters and Exit Criteria

- 5.5.1. The System Response Time used herein refers to the elapsed time between a user pressing a key to start a transaction and the first completed screen response containing the results or the appearance of the system prompt awaiting further user commands.

5.5.2. A transaction is defined as a completed unit of activity by a user of the System utilizing an on-line workstation interactively. The unit of activity is made up of one or more inputs by the users that result from input devices, such as a computer keyboard, barcode scanner or laser scanner. Upon processing of the input by the System, one or more characters of information response will be sent to the workstation that originated the input.

5.5.3. The Contractor shall comply with the performance test parameters as stated in the table below.

Parameters	Value
Number of users at normal concurrent load factor	<u>One Hundred (100)</u> users
Number of users at peak concurrent load factor	<u>One Hundred and fifty (150)</u> users
Maximum Think Time*	Not more than <u>Twenty (20)</u> seconds for all transactions
Duration for Benchmark and Stress Tests	At least <u>Sixty (60)</u> minutes
Duration for Endurance Test	At least <u>Eight (8)</u> hours

* The think time varies based on the business process defined in performance tests and shall be determined during the development of the performance test plan.

5.5.4. As exit criteria, the Performance Test shall meet the response time of the System as stated in the table below.

Response Time			
S/N	Type of transaction/report	Exit Criteria (Benchmark Test)	Exit Criteria (Stress Test)
1	Online Update/ Query <ul style="list-style-type: none"> Online Update: User executes transaction online and enters information into the transaction screen. Query: User runs ad-hoc query online. 	<ul style="list-style-type: none"> Shall not exceed <u>THREE (3)</u> seconds for <u>NINETY per cent (90%)</u> of the transactions. Shall not exceed <u>FIVE (5)</u> seconds for the remaining <u>FIFTY per</u> 	<ul style="list-style-type: none"> Shall not exceed <u>FIVE (5)</u> seconds for <u>NINETY-FIVE per cent (95%)</u> of the transactions. Shall not exceed <u>FIVE (5)</u> seconds for the next

Response Time			
S/N	Type of transaction/report	Exit Criteria (Benchmark Test)	Exit Criteria (Stress Test)
		<p><u>cent (50%)</u> of the transactions.</p> <ul style="list-style-type: none"> The above response time should be sustained up to the expected number of concurrent users for the System as specified in Clause 5.1.1. 	<p><u>FIFTY per cent (50%)</u> of the transactions.</p> <ul style="list-style-type: none"> The above response time should be sustained up to the expected number of concurrent users for the System as specified in Clause 5.1.1.
2	<p>Background Report (activated by user)</p> <ul style="list-style-type: none"> User executes report online but selects it to run as a background job. When this option is chosen, user can use the same session to perform other tasks while the report is being processed in the backend. 	<ul style="list-style-type: none"> Shall not exceed <u>THIRTY (30)</u> seconds for <u>EIGHTY per cent (80%)</u> of the reports. Shall not exceed <u>SIXTY (60)</u> seconds for the remaining <u>TWENTY per cent (20%)</u> of the reports. 	Not applicable
3	<p>Online Reports</p> <ul style="list-style-type: none"> User executes the report online. 	<ul style="list-style-type: none"> Shall not exceed <u>TWO (2)</u> minutes for <u>EIGHTY per cent (80%)</u> of the reports. Shall not exceed <u>TEN (10)</u> minutes for the remaining <u>TWENTY per cent</u> 	<ul style="list-style-type: none"> Shall not exceed <u>TWO (2)</u> minutes for <u>FIFTY per cent (50%)</u> of the reports. Shall not exceed <u>FIFTEEN (15)</u> minutes for the next <u>FORTY per cent (40%)</u> of

Response Time			
S/N	Type of transaction/report	Exit Criteria (Benchmark Test)	Exit Criteria (Stress Test)
		<u>(20%)</u> of the reports.	the reports.
4	Universal Search	For Search of data within the System that does not involve API calls: <ul style="list-style-type: none"> • Shall not exceed three (3) seconds for ninety (90) % of the time. • Shall not exceed five (5) seconds for ninety-five (95) % of the time. 	

- 5.5.5. The System shall be fault tolerant. An example of fault tolerance is the System's ability to handle graceful degradation of the system performance beyond the minimal performance requirements.
- 5.5.6. As far as System Performance is concerned, the Tenderer shall review the existing network infrastructure requirement and satisfy itself that the required response time could be met. The Tenderer shall highlight to the School, in detail, all necessary actions required for the existing network infrastructure, if according to its expert opinion, the existing network infrastructure could not satisfy the performance requirements. Failing which, the Tenderer shall bear all costs required to achieve the required response time.
- 5.5.7. The Contractor shall ensure that all 'batch processes' are completed within the designated batch window. The Contractor may choose to recommend the execution of certain batch processes to be performed during the daily Operating Hours, provided that they do not in any way affect the performance of the on-line operations.
- 5.5.8. The Contractor shall fine-tune the System when necessary, as requested by the School or when the Contractor deems that tuning is required, to ensure that the System meets the performance standards as specified in this Tender.

6. SYSTEM MAINTENANCE AND SUPPORT SERVICES

6.1. Overview

6.1.1. The Contractor shall provide the following types of application maintenance and support services:

- (a) Full Maintenance Support;
- (b) Ad-Hoc Support;
- (c) Database Administration and Support;
- (d) Middleware Administration and Support; and
- (e) Application Helpdesk.

6.1.2. The Contractor shall provide a maintenance team that is based in Singapore. As part of the maintenance contract, the Contractor shall allow the appointed School personnel to seek advice on software and hardware problems related to the System through communications means such as voice, video, email and meetings.

6.1.3. The Contractor's team assigned to the School is required to have at least **TWO (2) years** of relevant technical expertise and working experience to deliver the System.

6.2. Full Maintenance Support

6.2.1. The Contractor shall provide application maintenance and support services. The services covered in the base charges shall include:

- (a) Overall responsibility for the successful planning, transition, implementation and maintenance of on-going smooth operations of the entire System;
- (b) Work with designated School representatives to plan for and support identified School's operations (i.e. Financial Year-end Closings, Monthly payroll runs and etc.) that are dependent on the smooth operations of the System.
- (c) Provide System support services, including technical advice and assistance to ensure the continuity and availability and accessibility of the System;
- (d) Clear end-to-end accountability and commitment to the School;
- (e) Manage, support and implement, at the request of the School, Service Requests, for the purpose of operational enhancements and system upgrade in accordance to the requirements stated herein;

- (f) Administer and setup the UAT environment and assist users to load data to facilitate testing, when required;
- (g) Manage risks, investigate and rectify defects in the System as reported within the service level so as to minimise operational disruptions and/or business impacts. The effort includes resolving errors through developing, testing and implementing changes to the System;
- (h) Provide corrective maintenance, troubleshoot and isolate defects, including diagnosis and correction of all latent errors in the System. These include attending to user queries and provide support to them in the daily operations of the System;
- (i) Perform system testing of any fixes, upgrades, security patch;
- (j) Ensure data integrity and efficient performance;
- (k) Monitor, schedule and ensure successful completion of ad-hoc, daily, weekly, monthly and other batch reporting and processing jobs in the System;
- (l) Assess impact of new releases, upgrades or patches of system software to the System;
- (m) Ensure that all modifications to the System are properly integrated with the necessary components and that the System performance shall not be degraded;
- (n) Recover lost data, restore and repair damaged data and correct erroneous data to the extent possible;
- (o) Managing and supporting changes to the System to minimize impact on system availability;
- (p) Implement and enhance operational procedures as and when needed;
- (q) Update technical and user documentation for the System on soft copy;
- (r) Ensure that all program source codes and executable codes are properly maintained and backed up. Version numbers should be accurately documented. This is to allow the System to be rebuilt if required;
- (s) For problems that require third party Contractors or external organisations for troubleshooting and rectification, the Contractor shall act as a single point of contact for the School and follow through with the third-party Contractors. These third-party Contractors shall include any other Contractors that provide a service or a product that has relevance to the System;
- (t) Ensure that the System meets the data security requirements;

- (u) Prepare technical feasibility proposal including impact analysis, when requested by the School;
- (v) Implement and enhance operational procedures as and when needed;
- (w) Provide support for any system security review and audit activities and implement follow-up actions recommended by auditors/consultants to maintain and enhance the security of the System;
- (x) Provide and improve operational efficiency of the System through answering various system queries as deemed necessary when requested. This serves as part of the base maintenance support for the System;
- (y) Plan and propose continual improvement of the System, interfaces with internal and/or external systems, as well as the end-user computing environment, with the view to improve system efficiency and performance;
- (z) Propose improvements to the current work processes and procedures, which may result in faster turn-around time and increased efficiency in delivering the Services; and
- (aa) The Contractor shall propose and implement the following types of regular housekeeping:
 - (i) . Provide impact assessment on the removal of unused or outdated data tables before performing housekeeping of data tables;
 - (ii) Perform housekeeping of unused media files; and
 - (iii) Perform housekeeping of unused web pages, stylesheet, JavaScript and old version of middleware files.
 - (iv) Perform data archival in accordance with the School Data Retention and Disposal Policy.

6.2.2. The Contractor shall provide remedial support during the Support Hours of the System for the correction of any failure or malfunction of the System. Upon receipt of notification from the users that the System has failed or is malfunctioning, the Contractor shall respond to the School within the service level as specified in **Clause 9.1.14**.

6.2.3. The School also performs disaster recovery maintenance activities every year. The disaster recovery maintenance activities are performed either on weekdays or weekends. The Contractor shall work on-site, provide support and liaise with the School to prepare the disaster recovery environment and test cases/scripts, to conduct the pre and post application and system testing with the School's department representatives, execute and implement the disaster recovery activities for the System, if applicable.

6.3. Ad-Hoc Support

- 6.3.1. Ad-hoc support refers to support requests that are not covered under full maintenance support. Ad hoc support could include services such as one-off testing, setup for new system functionalities or application development/support for special events.
- 6.3.2. The School shall raise Service Requests for the Contractor to carry out the ad-hoc support.
- 6.3.3. The response time and turn-around time for any Service Request under ad-hoc support shall be based on mutual agreement between the School and the Contractor.

6.4. Database Administration and Support

- 6.4.1. The Contractor shall be responsible for the day-to-day database administration, management, operations and deployments of all databases in the System during the contracted period.
- 6.4.2. The Contractor shall ensure that the System meets the performance standards in terms of response times, availability and data integrity. Refer to **Part 2 Clause 5** of this Tender Specifications for details.
- 6.4.3. The activities to be performed shall include the following:
- (a) Logical and physical database design and creation, changes or removal of database, provide technical consultancy and advice on the usage of database software, advise application developers and owners on optimisation of database usage, SQL code, etc and monitor availability of database, listener and other related processes;
 - (b) Improve and enforce database standards and procedures to achieve optimum database performance;
 - (c) Monitor and analyse the disk storage usage of all production databases including database objects such as table space, index space, etc. and alert users promptly of potential application failure due to data out-growing the allocated space etc. to pre-empt problems. E.g. oversized log files etc.;
 - (d) Monitor database space utilisation and predict growth;
 - (e) Review all daily logs, database alerts, database export logs, scheduled job logs, etc.;
 - (f) Investigate and report to the School of any exceptions or abnormal events and the preventive actions implemented;
 - (g) Monitor database health and performance;

- (h) Tune database to maintain database in healthy and optimum data size state;
- (i) Perform weekly diagnosis on the databases to ensure data integrity and proper functioning of the databases;
- (j) Once approved by the School, the Contractor shall perform data patching whenever required to correct any data corruption errors;
- (k) Perform database re-organization at least on a quarterly basis, when required;
- (l) Generate monthly reports to inform all application developers and owners about the database utilization of the application, for necessary actions to be taken by the latter. The Contractor shall also generate monthly reports on connections utilization on database of the application;
- (m) Monitor and analyse the connections and sessions usage of all databases and alert users promptly of application failure. The Contractor shall also advise the School on changes required;
- (n) Perform database backups at the frequency and within the timeframe as specified by the School;
- (o) Perform database recovery within the timeframe as defined by the School;
- (p) Perform annual database recovery test on selected databases as determined by the School.

6.4.4. The Contractor shall be responsible for the management (includes development, maintenance and improvement) of all customised scripts, programs and tools to automate and enhance the efficiency of the database administration and operations.

6.4.5. The Contractor shall develop, review, test, implement and monitor database backup and recovery jobs, procedures and schedules.

6.4.6. The Contractor shall plan and schedule regular database housekeeping and maintenance activities necessary to keep the database in a healthy state and at optimum performance.

6.4.7. The Contractor shall carry out installation and configuration of new databases, re-installation and re-configuration of existing databases and configuration of database connectivity as instructed by the School.

6.4.8. The Contractor shall perform database management software maintenance to ensure that it remains functional and that it remains at a supportable level.

- 6.4.9. The maintenance includes refreshing a software product, bringing a software up to current level of maintenance by applying maintenance fixes and service packs, testing and verifying the impact of new products, perform minor software upgrade etc. In addition, the Contractor shall:
- (a) Keep track of availability of all database updates and patch releases by the database vendors;
 - (b) Analyse, assess impact and recommend the relevant patches available to the School; and
 - (c) Be responsible for all upgrades, installations, testing to ensure compatibility and application of all necessary patches.
- 6.4.10. The Contractor shall co-ordinate the entire patch application effort, which includes:
- (a) Planning;
 - (b) Co-ordination with the application services team(s) and third-party vendors appointed by the School;
 - (c) Preparation and update documentation; and
 - (d) Execution of the plan according to the schedule as agreed with the School.
- 6.4.11. The Contractor may propose suitable mechanisms and procedures to facilitate more efficient database administration and management to the School for consideration and approval.
- 6.4.12. The Contractor may propose the use of tools to automate the administration and maintenance of database accounts subject to the School's approval.
- 6.4.13. The Contractor shall be responsible for database deployment tasks include the following:
- (a) Database objects deployment (e.g. Creation/ modification /deletion of database object);
 - (b) Scripts deployment;
 - (c) Scripts execution; and
 - (d) Data extraction.
- 6.4.14. The Contractor shall adhere to the School's current mechanisms, controls and procedures to carry out the necessary database deployment tasks.
- 6.4.15. The Contractor may propose suitable mechanisms and procedures to facilitate more efficient and effective database deployment to the School for consideration and approval.

- 6.4.16. The Contractor shall ensure that the administration and management of database functions do not compromise the security of any of the databases.
- 6.4.17. The Contractor shall review database audit trails daily and investigate (if necessary) and report to the School of any access violations, exceptional, unauthorised or suspicious activities and potential problems.
- 6.4.18. The Contractor shall ensure that all database related documentation on the set-up, environment, configuration, patch levels, etc are kept up-to-date.
- 6.4.19. The Contractor shall also update and maintain all documentation on procedure related to the database administration, maintenance deployment functions.
- 6.4.20. The Contractor shall be responsible for the administration and maintenance of database accounts for all databases.
- 6.4.21. The tasks include maintenance and deletion of database accounts and privileges, resetting of passwords, etc.
- 6.4.22. The Contractor shall adhere to the existing mechanisms, standards, controls and procedure to carry out the necessary database account management tasks.
- 6.4.23. The Contractor may propose suitable mechanisms and procedures to facilitate more efficient and effective database account management to the School for consideration and approval.

6.5. System Maintenance and Support Plan

- 6.5.1. The Contractor shall produce and maintain a detailed System Maintenance and Support Plan **ONE (1) month** prior to the date of System Commissioning, showing the scope of work, contacts, deliverables and implementation strategies. The System Maintenance and Support Plan shall be approved by the School.
- 6.5.2. The Maintenance and Support Plan shall minimally cover the following areas:
- (a) Project team structure;
 - (b) Roles and responsibilities;
 - (c) Approach to manage and execute the maintenance and support of the System;
 - (d) Dates of all identifiable activities;
 - (e) Methodologies, procedures, standards, practices and conventions to be applied; and
 - (f) Escalation Matrix in the case of defects.

6.5.3. The System Maintenance and Support Plan shall include activities to be carried out by the School, as well as all other personnel whose actions are required. The System Maintenance and Support Plan shall include a diagram depicting the reporting structure and the key support personnel who shall be involved in the support services. It shall define clearly the roles and responsibilities of all personnel assigned by the Contractor and how each project team shall interact with one another to deliver the desired services.

6.5.4. The Contractor shall maintain the System Maintenance and Support Plan during the system maintenance phase after the delivery of the System.

6.6. Middleware Administration and Support

6.6.1. Middleware administration and support for the System shall include the following:

- (a) Investigation and correction of defects in the Middleware as reported by the School including temporary corrections and bypass of the defects until such time as standard corrections and/or updates of the Middleware are available ("Remedial Support");
- (b) Installation, testing and the implementation of standard corrections, updates, supply and installation of new versions and new releases of the Middleware and updating of related documentation and materials;
- (c) Render advice on the performance tuning of all items of the middleware;
- (d) Restore the System to an operable state where System Downtime is attributable to Middleware defect or error;
- (e) Render advice and guidance to the School on the use of the Middleware;
- (f) Inform the School of all future updates and new releases of the Middleware within TWO (2) calendar weeks of their release for general distribution and, when so requested by the School, supplying and installing the relevant update and releases within FOUR (4) calendar weeks of receipt of the School's request; and
- (g) Provide other Middleware support services including technical advice and assistance as may be required by the School from time to time.
- (h) Administer the middleware such as managing services, configuration, and troubleshooting.

6.7. Application Helpdesk

- 6.7.1. The School has a helpdesk to provide support for its users for incidents reported, which may include troubleshooting IT problems encountered (e.g. School issued end-user devices, desktop, agency network and account authentication, firewall, and 1st level support for selected agency applications).
- 6.7.2. The Contractor shall provide an Application Helpdesk for the School's users on issues related to the System, during the System Warranty Period and Maintenance Period.
- 6.7.3. The Contractor may receive a request for support services (i) as an incident escalated from any school's helpdesk or (ii) directly from any School's user. The Contractor shall ensure that the System allows the School's users to request for support services directly from the Application Helpdesk. Where the Contractor receives a request for support services directly from any School's user, the Contractor shall interact directly with School's users and provide all the necessary supports.
- 6.7.4. The Contractor shall ensure that its Application Helpdesk team provides a single point of contact to handle all support matters and provide Maintenance Services during the Support Hours.
- 6.7.5. The Contractor shall ensure that its Application Helpdesk meets the following requirements:
- (a) must be located in Singapore; and
 - (b) must centrally log, track and monitor till closure all requests for support services and resolve all problems and issues in accordance with the service levels stipulated in the Contract.
- 6.7.6. The Contractor shall submit to the School a monthly helpdesk report of all reported problems. The report shall include the following performance indicators and statistics:
- (a) the number of tickets raised, resolved or outstanding for the month, in total, per severity, per category, per modules, per sub-modules and per cause;
 - (b) the trend of the tickets, in comparison to prior months and years;
 - (c) the aging profile of all outstanding tickets;
 - (d) the Resolution Time and service levels;
 - (e) the Change Request and Service Request statistics, trends and outstanding/aging requests based on status, module, the Licensees; and
 - (f) any other statistics to enable the School to track the healthiness of tickets.

6.8. Standards and Procedure

6.8.1. The Contractor shall document and maintain comprehensive application related standards and guidelines so as to ease maintenance of the System. The guidelines shall include:

- (a) Integration / Interface standards;
- (b) System flow standards;
- (c) User interface standards and guidelines (including consistent error messages);
- (d) System related naming conventions (e.g. Programs);
- (e) Migration control procedures;
- (f) System security invocation standards and guidelines; and
- (g) System common utilities invocation standards and guidelines.

6.8.2. The Contractor may propose to adopt its system-related standards and guidelines (if such are available) and supply them together with the Tender proposal. The School shall reserve the rights to adopt such standards and guidelines.

6.9. Maintenance Log

6.9.1. The Contractor shall maintain a log of all maintenance activities, including corrective maintenance and other services. For each activity, the log will record minimally, the date, time, details of the fault or problem, corrective and follow-up action, and the names of the service personnel involved in the activity. The Contractor shall propose a format of the Maintenance Log and recommend procedures for its usage within 2 weeks after commencement of contract. The format and recommended procedures for the Maintenance Log shall be subject to the School's approval.

7. SUPPORT HOURS AND OPERATING HOURS

7.1. Overview

- 7.1.1. The Support Hours for the System shall be 8.00 a.m. to 8.00 p.m. from Mondays to Fridays, exclude Saturdays and Sundays and Public Holidays.
- 7.1.2. The Operating Hours for the System shall be **TWENTY-FOUR (24)** hours a day, **SEVEN (7)** days a week, inclusive of Sundays and Public Holidays. The System shall be fully operable during the Operating Hours.
- 7.1.3. The Contractor's Project Manager and Team Lead shall be contactable at all times via mobile phone. The Contractor's personnel may be activated after office hours to resolve critical problems.
- 7.1.4. Upon notification of the problem, the Contractor's personnel must respond within the required response time specified in **Clause 12.8.8** during the support hours of the System.
- 7.1.5. The Contractor shall continue to provide support services after the support hours, at no additional cost to the School, for resolution of Severity Level **HIGH, and MEDIUM** problem and restoration of the system in the event of any failure.
- 7.1.6. For Severity Level **HIGH, and MEDIUM** problems, the Contractor shall ensure that the System is operational within the stipulated recovery time stated in **Clause 9.1.18**. This includes weekends and public holidays.

8. SERVICE REQUESTS

8.1. Overview

- 8.1.1. The Contractor shall implement at the request of the School, all Service Requests for enhancement to the System.
- 8.1.2. The Tenderer shall propose a standard¹ man-day rate for all Service Requests during the contracted period. All prices quoted shall be in accordance to the formats specified in **Part 5**.
- 8.1.3. The School shall procure the man-days, through the issuance of Purchase Order(s)/ written notification(s)/ other formats, as and when Service Requests are confirmed. As a guide, the annual Service Request man-days is estimated for 100 man-days with any unused man-days in a year to be rolled over to the following year. The Contractor shall make its assessment and propose the optimal manpower needed to meet the service level of this contract.
- 8.1.4. The Contractor shall only bill the School monthly on the Service Requests that are implemented and accepted by the School. The conditions for acceptance of the Service Request are listed in **Clause 8.4.4**.
- 8.1.5. The School shall be under no obligation to purchase any of the Services specified in the Contract Period except to the extent of the Purchase Order(s)/ written notification(s)/ other formats for those Services issued by the School.
- 8.1.6. The Contractor shall have the resources to service up to three (3) Service Requests concurrently when required.
- 8.1.7. The Contractor's scope of work for service request shall include the following:
- (a) Make an assessment on the Service Request and submit reports to the School for approval. The study shall detail the impact analysis and will be considered as part of the operations support and therefore not chargeable;
 - (b) Carry out design, programming and testing work to modify the System in order to meet requirements of the Service Request;
 - (c) Propose wireframes and prototypes, low and high-fidelity mock-ups for usability testing. Wireframes and prototypes should be based on the understanding of business requirements and analyzing user behavior, after which using storyboard, process flows and sitemaps to illustrate designs. Graphic user interface (GUI) components like menus, tabs, buttons, etc. shall be designed based on Singapore Government Design System or equivalent standards.

¹ The standard rate is the blended rate of Project Manager and all levels of developers, system engineers and database administrators.

- (d) Support the unit testing, system integration testing, interface testing and user acceptance test of all service request e.g. conduct pre-UAT briefing, demonstration, prepare the required test data (volume and criteria to be determined by the School), test scenarios, test cases, test plan, update the defect consolidated logs, set up the testing environment(s), etc.;
- (e) Implement proper version control management on all changes / enhancements and implement the changes / enhancements to the production environment successfully;
- (f) Handover the system to Operations;
- (g) Train the School's users on the changes to enable them to be competent and self-reliant in the operations of the System after the changes; and
- (h) Prepare / update relevant documentation to reflect the changes made to the System, etc.

- 8.1.8. The Contractor shall work with the School to prioritise the Service Requests accepted. The School reserves the right to re-prioritise any Service Requests given earlier and the School shall not be liable for any additional costs thereby incurred.
- 8.1.9. The Contractor shall note that changes made to the System such as implementation of system patches, security patches or bug fixing, fine-tuning of application systems for better performance, etc, shall not be addressed through the Service Request mechanisms. All such changes are termed as production support and shall be included as part of the Base Services.
- 8.1.10. All design, development / customisation changes and impact analysis shall be identified and recorded, verified and validated by the Contractor and submitted to the School for review and approval before implementation. The results of the review of changes and subsequent follow up actions shall be documented as part of the Quality Records at no additional cost to the School.
- 8.1.11. The Contractor is responsible for ensuring that accepted Service Requests are successfully implemented according to agreed schedule based on agreed man-effort. The Contractor shall comply with the agreed schedule strictly, even if this would include working beyond normal working hours. The School shall not be liable for any additional costs incurred by the Contractor under this Clause.
- 8.1.12. The Contractor shall note that the computation of the Elapsed Completion Time starts upon approval of the SR proposal by the School.
- 8.1.13. The Contractor shall ensure that User Acceptance Testing (UAT) is conducted satisfactorily for SR. The users shall not be required to conduct more than **TWO (2) rounds** of UAT, unless requested or required by the users.
- 8.1.14. The Contractor shall produce monthly reports on all SR raised, their respective status and progress.

8.2. Service Request Procedure

8.2.1. The Contractor shall refer to the School's Change Management Procedure.

8.2.2. The Service Request Control Procedure that the Contractor shall undertake includes the following activities:

- (a) Estimate the resource costs, detail the impact of changes to the application such as system performance, system integration, system availability, and elapsed time for implementing the change;
- (b) Define and make specific changes to the applied modules of Software, hardware elements (if any) and the documentation;
- (c) Provide sign-off for system testing to prove completion of the necessary changes, unit testing, technical review conducted by a peer or technical lead and system integration testing before releasing the changes for user acceptance testing (UAT);
- (d) Provide UAT test plan, test scenarios, test base, set up UAT environment and conduct pre-UAT briefing, walk-through and demonstration to users where applicable. If the Service Request needs more than **TWENTY (20) man-days** to complete and involves a change in functionality in the System, the Contractor has to produce a thorough Test Plan;
- (e) Support the user acceptance testing, rectifying any problems reported promptly and documenting the defects reported and resolved during the user acceptance testing period;
- (f) Obtain approval from the School for migration of changes into the production environment;
- (g) Provide forms, scripts for all program migrations to UAT and production environments;
- (h) Ensure that all work carried out must not jeopardize the System, systems' availability, performance, confidentiality, data integrity, data confidentiality and security;
- (i) Monitor the System after post implementation of changes to ensure operations are not being affected;
- (j) Train users on the system changes to enable them to be competent and self-reliant in the operation of the System;
- (k) Appoint Quality Assurance (QA) Officer to review all deliverables provided to the School.
- (l) The QA officer shall not be the developer.

8.3. Service Request Service Levels

- 8.3.1. In addition to complying with the School's Service Request Control Procedure, the Contractor shall ensure that all Service Requests are assessed, completed and implemented; comply with the given timeframe as shown in the table below. The Contractor shall submit the impact analysis on the assessment of effort and Turnaround Time within the following timeframe for the various types of service request.

Table 1:Service Requests (SR) Timeframe

Estimated SR Man-days Effort	Assessment of effort and Impact Analysis (From the day the service request is raised to the day that the assessment of effort is provided such as impact analysis and resource estimation for the SR)	Turnaround Time (From the day the service request is approved to the day the service request is completed)
SR that requires more than TEN (10) man-days to complete	Mutually agreed timeframe	Based on mutual agreement between the School and the Contractor
SR that requires more than FIVE (5) man-days but less than or equal to TEN (10) man-days to complete	Within FIVE (5) working days	Within TWELVE (12) working days
SR that requires less than or equal to FIVE (5) man-days to complete	Within THREE (3) working days	Within SEVEN (7) working days
SR that requires less than or equal to ONE (1) man-day to complete	Within ONE (1) working day	Within THREE (3) working days
Urgent SR	Within ONE (1) working day	Within THREE (3) working days or Mutually agreed timeframe for all urgent SR.

- 8.3.2. The School reserves the right to raise urgent Service Requests. The Contractor shall complete assessment effort of such requests within ONE (1) working day of receipt of the urgent Service Request. The turnaround time of urgent Service Requests shall be within THREE (3) working days from the day the request is approved to the day the request is completed. Any deviation shall be mutually agreed between the School and the Contractor.
- 8.3.3. All efforts spent in the assessment of impact of service requests shall be accounted for under operations support and non-chargeable. All man-efforts assessment is subjected to the approval of the School.

- 8.3.4. The aim of the Service Request Management is to ensure that all proposals for any changes to the System are properly evaluated in terms of their priorities, costs and benefits. Such changes include amendments to the system documentation and operational procedures.

8.4. Turnaround Time

- 8.4.1. All accepted requests shall be completed and implemented within the specified turnaround time depending on the estimated man-days required.
- 8.4.2. The Contractor is responsible for ensuring that Service Request is successfully implemented according to agreed schedule based on agreed man-efforts. The Contractor is expected to work beyond normal working hour if they cannot meet the pre-agreed schedule and such additional costs incurred shall be borne by the Contractor.
- 8.4.3. The Contractor shall note that the implementation of a Service Request may be carried out on a one-time basis or in phases, to be specified by the School.
- 8.4.4. A Service Request shall be considered as successfully completed by the Contractor after the following conditions are met:
- (a) Completed User Acceptance Test;
 - (b) Contractor's work has been accepted by user;
 - (c) All relevant documentation is prepared/updated and accepted by the School; and
 - (d) Enhanced/new system has been cutover to production environment.
- 8.4.5. For phased implementation, the System can be cutover to production environment in phases. The Service Request would be considered completed after all application programs have been successfully migrated to the production environment and when all relevant documentation is prepared / updated and accepted by the School.

9. PROBLEM ESCALATION, ANALYSIS, RESOLUTION AND MANAGEMENT

9.1. Problem Management

- 9.1.1. The Contractor shall note that this Clause is applicable during the Performance Guarantee Period (PGP) and the maintenance period.
- 9.1.2. The Contractor shall provide Application Helpdesk after the Commissioning of the System. The Application Helpdesk personnel shall have good knowledge and understanding of the System and the School's environment. The Application Helpdesk shall be the single point of contact for enquiries and problem reporting, escalation, tracking and resolution.
- 9.1.3. The Contractor shall complete training the School's Helpdesk staff FOUR (4) calendar weeks before the System Commissioning to provide necessary basic user support if required. The Contractor shall also provide them with clear documentation such as FAQs on carrying out the support during the training.
- 9.1.4. On a quarterly basis, the Contractor shall review all the problems logged and update the documentation such as FAQs
- 9.1.5. The Contractor shall respond to all escalated service calls from the School during the Support Hours.
- 9.1.6. The Contractor shall take full ownership of all problems related to the availability of the System; regardless the cause is related to hardware, software, application or data. In the case that the problem is traced to component(s) not supplied by the Contractor, the Contractor shall work with the Hardware vendors, Software vendors, the School's vendors, the other School / School Contractors, and the Contractor's vendors closely to identify the real problem cause and ensure that the problem is resolved, within the stipulated turnaround time. Such support from the Contractor shall be part of the base maintenance services for the System and hence carried out at no additional cost to the School.
- 9.1.7. When problems are encountered such that the System needs to be shut down as part of the problem resolution, the Contractor shall schedule the ad-hoc downtime after the Support Hours of the System, subject to the School's approval.
- 9.1.8. The Contractor shall escalate the cases to the relevant parties for action and track the status of cases periodically until closure. The Contractor shall coordinate all activities by working with the respective Contractors appointed by the School to ensure that all escalated cases are resolved according to established service level agreements.
- 9.1.9. The Contractor shall take ownership to ensure that problems reported are resolved promptly and within defined service levels for different problem severity levels regardless of the cause of the problem.

- 9.1.10. The Contractor shall keep the School's updated on status of each problem.
- 9.1.11. The Contractor shall note that all calls that are referring to the same problem shall be logged as a single case.
- 9.1.12. The Contractor shall ensure that a problem shall be deemed closed only after the person who reported the problem has acknowledged that no further follow up action is required.
- 9.1.13. The classification of the defect or errors in the System is specified below:

Table 2: Classification of Severity Levels

Severity Level	Nature and impact of the incident	Examples of Incidents
High	<ul style="list-style-type: none"> • Damage (including reputational damage) to the School • Temporary and minor emotional distress or disturbance to the individual • Reduction in competitiveness or a compromise of business interests 	<p><u>A) Impact on Business Operations</u></p> <ul style="list-style-type: none"> • Unavailability of System or unavailability of a critical module or unavailability of part of the System disrupting service wide central service; or • Disruption of the operations of a user(s) or halting a time-critical system or affecting the majority of users (>20%); or • Error in a public facing module that may potentially result in a negative image or adverse impact on the reputation of the School; or • Disruption caused by any third party service (e.g. NETS, Banks) that affects the System; or • Issues that affect any key business process that is time critical (e.g. journal postings and Ranking and Promotion exercise); or • Issues or Problems with Payroll processing and bonus payment that affect the majority of users (>20%); or • Issues or Problems with IRAS or CPF processing (e.g. generation of files, excluding transmission related problem) or any other statutory processing requirements; or • Issues that affect any self-service module. <p>OR</p> <p><u>B) Effects on Key Decision-Making Users</u></p> <ul style="list-style-type: none"> • Issues affecting key decision making users (e.g. senior management).

Severity Level	Nature and impact of the incident	Examples of Incidents
		<p>OR</p> <p><u>C) Security Breaches of School Systems</u></p> <p><u>Malicious Security Attacks</u></p> <ul style="list-style-type: none"> Incidents affecting national level (denial of service, targeted attacks, sabotage, etc.) System; or Incidents that may potentially affect the ability of the School to perform its function; or Incidents that are localised within businesses that may have an adverse impact on the business operations of that businesses users. <p><u>Web Defacement</u></p> <ul style="list-style-type: none"> Incidents that affect the School's Internet or Intranet site, with potential to result in negative image or adverse impact on the reputation of the School. <p><u>Virus/Worm/Trojans</u></p> <ul style="list-style-type: none"> Virus attacks that disrupt System services resulting in adverse impact on the business operation of the users.
Medium	<ul style="list-style-type: none"> Difficult or undesirable consequences to the School Minor inconvenience to individuals or businesses 	<p><u>A) Impact on Business Operations; or</u></p> <ul style="list-style-type: none"> Disruptions affecting small groups of users (<20%) or affecting only a particular process, System or function of the users, where alternatives or temporary workaround solutions or bypasses are available; or Problems affecting the QA environment or training environment; or Disruptions affecting the School's System which are not time-critical or where existing alternatives are available. <p><u>B) Security Breach of the System; or</u></p> <p><u>Malicious Security Attacks</u></p> <ul style="list-style-type: none"> Targeted attacks on School resulting in some impact on the School's ability to perform its function; or Incident localised within a businesses but which has no adverse impact on the business operation of the businesses user. <p><u>Virus/Worm/Trojans</u></p>

Severity Level	Nature and impact of the incident	Examples of Incidents
		<ul style="list-style-type: none"> • Localised attack disrupting any user within a businesses with some impact on businesses operation; or • Virus attack affecting one businesses but resulting in no adverse impact on the business operation. <p><u>C) System Response</u></p> <ul style="list-style-type: none"> • Failure of the System to meet the System Response Time required under Part 2B Section 7 (System Performance, Availability and Reliability).
Low	<ul style="list-style-type: none"> • Minimal impact on the School , individuals, or businesses 	<p><u>A) Impact on Business Operations; or</u></p> <ul style="list-style-type: none"> • Defects or problems that affect a particular area of operations but do not affect any operational objectives as there exists temporary workaround solutions; or • Defects or problems that have minimal or no effects on operations and do not affect any operational objectives; or • Disruption of services that have minimal or no impact on the a users' ability to perform their function; or • Problems affecting the UAT environment or development environment. <p><u>B) Security Breaches of the System</u></p> <p><u>Malicious Security Attacks</u></p> <ul style="list-style-type: none"> • Unsuccessful attempts to attack as reported from scans and probes, spoofing of emails, spam/scam emails etc. <p><u>Virus/Worm/Trojans</u></p> <ul style="list-style-type: none"> • Incidents affecting a user within a Licensee that have no impact on the Licensee's operations.

9.1.14. The service level for each classification of the incident, defect or errors in the System is classified and specified in **Clause 12.8.8:**

9.1.15. The Severity Level, which measure the overall impact of the problem, shall be jointly assigned based on the four criteria shown below:

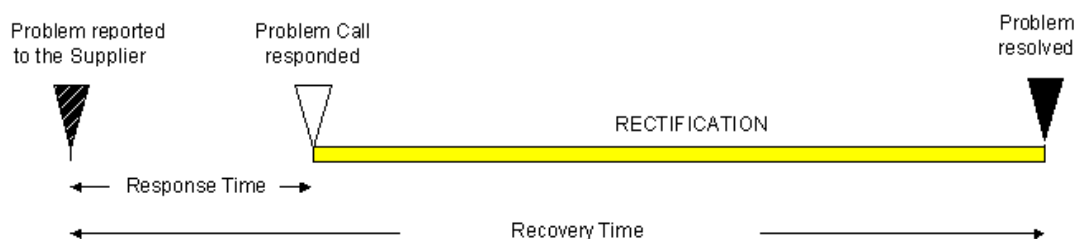
- (a) Number of users affected;
- (b) Availability of a bypass or fallback;
- (c) Type and extent of service disrupted; and
- (d) Extent of business and operation impact.

9.1.16. The School shall have the final decision on the severity level, and this shall be conclusive and binding to all parties involved in resolving the problem / defect.

9.1.17. There are 2 measurements: Response Time and Recovery Time:

Severity	Description
Response Time	<p>The Response Time shall begin from the time or date the problem / defect is communicated to the Contractor's single point of contact, regardless of whether the single point of contact acknowledges receipt of the message.</p> <p>The Response Time ends when a response is provided by the Contractor via telephone or electronic mail to the person who reported the problem / defect.</p>
Recovery Time	<p>Recovery Time shall begin upon communication of the problem / defect to the Contractor's single point of contact, regardless of whether the single point of contact acknowledges receipt of the message.</p> <p>The Recovery Time ends when the root cause of the problem / defect is resolved and the System is restored to the satisfaction of the School.</p>

Figure 2: Illustration of Response Time and Problem Resolution Time



- 9.1.18. The Contractor shall update the School on the progress of the incident based on the schedule as shown in **Clause 12.8.8** after the resolution is accepted by the School.
- 9.1.19. The Contractor shall provide a mechanism and substantiate to the School that Service Levels are met. There shall be proper acknowledgement and monitoring of all reported defects and problems by the Contractor. The Contractor shall be responsible for ensuring that the representative of the School is kept updated on the latest status of the reported defects or problems without being prompted. The Contractor shall ensure that all root cause of the problem(s) reported, regardless of severity, be resolved within TWO (2) calendar weeks.
- 9.1.20. The Contractor shall track, monitor and report on the reported problems. The information required to be captured shall include at least the following:
- (a) Problem Reference Number;
 - (b) Problem Description;
 - (c) Problem Severity Level;
 - (d) Caller's Details;
 - (e) Date and Time of Report;
 - (f) Date and Time at which Contractor Respond to Problem;
 - (g) Details of Vendor who Attended and Resolved Problem;
 - (h) Date and Time of Problem Resolution;
 - (i) Problem Cause to its Component Level and Scope of Impact;
 - (j) Resolution Details;
 - (k) Preventive Recommendations / Remarks;
 - (l) Highlight problems that are not resolved; and
 - (m) The time taken to resolve problems of different severity level to ensure Service Levels have been met for the completion of all problem calls, etc.
- 9.1.21. For **All** Severity Levels problem, the Contractor shall inform the School immediately through escalation process and shall brief the School on the causes, area of impact and lead-time for recovery. The formal incident report shall be submitted in accordance with the schedule as specified in **Clause 12.8.8**. If an incident is prolonged, the Contractor shall be put up progress reports in accordance with the schedule specified in **Clause 12.8.8**.

- 9.1.22. The Contractor shall note that all incident reports shall not be sent to anyone other than those mentioned in the escalation list without prior approval from the School.
- 9.1.23. The Contractor shall take all measures necessary to ensure that the response time stated in **Clause 129.1.14** of this Tender Specifications is complied with and shall, if requested by the School, provide its personnel with mobile phones or any other equipment which the School may require to ensure that the response time is always complied with.
- 9.1.24. The Contractor shall inform the School of the contact persons and contact telephone numbers of its personnel to whom requests for Remedial Support shall be made. Any report of a problem in the System to any person nominated by the Contractor by name or to a person answering to a telephone number supplied by the Contractor pursuant to this Clause shall be deemed to be a request for Remedial Support contemplated by this Clause.
- 9.1.25. The School may from time to time request the Contractor to locate specific type of problems or Helpdesk calls logged by specific users. The Contractor shall be able to extract and print this information from the Problem Management System.
- 9.1.26. All problems / defects shall be tracked with detailed trending that contains information such as severity, priority, aging and status. There must be proper acknowledgement of all reported System errors and encountered problems and monitoring of the status of the reported errors and problems by the Contractor.
- 9.1.27. The Contractor shall also provide an analysis of the problems encountered and propose actions to prevent these problems from recurring, and pre-empt similar problems from occurring.
- 9.1.28. In the event of failure to meet the performance service levels, the Contractor shall provide additional qualified personnel and/or resources to rectify the situation at no additional cost to the School. In the event of a replacement or exit of personnel, the Contractor shall be responsible for training the successor and ensuring that the replacement staff is technically competent in continuing the work with no disruption to the performance of the service levels.

10. TECHNICAL REQUIREMENTS

10.1. General Requirements

10.1.1. The Tenderer shall provide a clear roadmap of the proposed SaaS illustrating its current capabilities and future enhancements in the Proposal. The information to be provided shall minimally cover the following:

- (a) Diagrams to illustrate the SaaS architecture.
- (b) Interfacing requirements between SaaS and other products.
- (c) Any specific storage / archival / restoration requirement.
- (d) The notice and approach to support upgrade of new releases, version and product end-of-support and extended end-of-support of the SaaS or any software or tools it interacts with.
- (e) Future major and minor releases, date of projected release and projected new functionalities of the software and tools proposed
- (f) The Contractor shall specify the release date and version of the proposed Software. If the new release to the Software is announced after the Letter of Acceptance has been issued, the Contractor shall offer the new version of the Software under the same terms and conditions as that set out in this Tender Specifications.
- (g) The proposed System shall be IPv4 and IPv6 compliant.

10.2. System Environment

10.2.1. The Contractor shall setup THREE (3) environments for the hosting of the System.

- (a) Production Environment (PROD);
- (b) User Acceptance Test (UAT); and
- (c) Development, Quality Assurance and Testing (QAT).

10.2.2. The UAT environment is the user acceptance and testing environment to the PROD environment. The UAT environment and design shall mimic the PROD environment but with reduced capacity.

10.2.3. The QAT environment is the development, quality assurance and testing environment to the UAT environment. The QAT environment and design shall mimic the PROD / UAT environment but with reduced capacity.

10.2.4. The Tenderer shall propose the sizing for the UAT and QAT environments and indicate the reasons for the sizing in comparison to PROD environment.

- 10.2.5. The Tenderer shall propose all cloud resources including the projected growth to support all the functions in the System and other enhancements. The Tenderer shall carry out capacity sizing for the application based on system availability requirements and current and projected future growth.
- 10.2.6. The Tender proposed solution shall meet the availability requirements stipulated in Table 1-1 to support the System's business continuity.

Table 1-1: Availability Requirements

Environment	Availability Requirements
PROD	As stipulated in Part 2 of the Tender Specification
UAT	95% - To facilitate applications on-boarding, functional and integration testing
QAT	95% - To facilitate applications development, functional, quality assurance and integration testing

10.3. Data Backup & Restoration

- 10.3.1. The Tenderer shall propose and implement a data backup and restoration strategy for the System that has a data lifespan in accordance with the School's Data Archival and Retention policy.
- 10.3.2. The Tenderer shall describe in detail how the data backup and restoration activities are performed.
- 10.3.3. The Contractor shall ensure the proposed data backup & restoration solution meet the School's prevailing Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
- 10.3.4. The backup and recovery plan shall cater for the recovery of all transactions, logs, and data from the most recent backup. Details shall at least include information such as data retention periods, frequency of backup, types of backup (such as incremental and full backup), what data to backup (such as application data files, system files), and the process of system recovery from the backups following a system failure and fallback procedures.
- 10.3.5. The Contractor shall submit a backup and recovery plan which shall be tested on the hosting environment for approval of the School no later than THREE (3) months before System Commissioning.

- 10.3.6. The Contractor shall ensure that the documentation remains up-to-date and all or any changes to the plan must be sent to the School for approval at least ONE (1) month before the changes are to be executed.

10.4. Development Facility Requirements

- 10.4.1. The Contractor shall provide a software development facility and environment for the development, unit testing, system testing, integration testing, defect rectification, and enhancement / upgrade of the System.
- 10.4.2. The purpose of this facility is also to isolate the above-mentioned activities from the actual production system for security reasons and better system resilience.
- 10.4.3. The Contractor shall bear all costs, expenses, charges, including transportation, insurance, additional software, etc associated with the project.
- 10.4.4. The Contractor shall ensure the confidentiality and integrity of the development facility and data provided by the School, if any.
- 10.4.5. The Contractor shall furnish detailed procedures to assure the School that the components of the System (e.g., documentation, program specifications, etc.) issued by the School are safeguarded against unauthorised access and are returned to the School upon termination of the Contract.
- 10.4.6. The Contractor's personnel shall perform the following services:
- (a) Requirement gatherings;
 - (b) Data conversion and migration;
 - (c) Migration and deployment of the System;
 - (d) User Acceptance Testing;
 - (e) Other testing (not inclusive of unit test and system test) e.g. System Performance Test, System restoration test, etc.;
 - (f) User Training;
 - (g) Meetings;
 - (h) Troubleshooting with the users; and
 - (i) Support monthly preventive maintenance activities.
- 10.4.7. Furnish details of a procedure to enable the transfer of source codes etc, from the Contractor's site to the School's designated premises for Acceptance Testing.

- 10.4.8. The School shall reserve the right to inspect the development facilities at the Contractor's premises at any point of time.

10.5. System Architecture

- 10.5.1. The Tenderer shall provide description and diagrams of the system architecture proposed. The diagram shall include, at least, sequence diagram(s), state or collaboration diagram(s) and component diagram(s) that will form implementation view of the System.
- 10.5.2. The system architecture describes logical components used, the relationship between the components and how components are deployed in the System. The logical components shall include new services (if any), hardware, software, interconnections and interfaces with existing environment and any other resources used. The Tenderer shall include the advantages and disadvantages of the proposed architecture.
- 10.5.3. The Contractor shall brief the proposed system architecture to the School upon award.
- 10.5.4. The system architecture shall be subjected to the School's approval.
- 10.5.5. The Contractor shall consider the use of tools to support pattern and transformations for automating refinement of models and transition between analysis, design and implementation.
- 10.5.6. If the Contractor chooses to use proprietary software, the Contractor shall ensure that they are able to maintain this software throughout the lifespan of the System. If such cases arise, the Contractor shall inform and seek the School for approval.
- 10.5.7. The proposed design and architecture of the System shall be reviewed by the product principal and/or CSP. The Tenderer shall submit evidence of review and authorised partner/reseller of the product(s), where applicable together with the tender submission.
- 10.5.8. Tenderer shall ensure that dedicated Program Architect Assurance service contract with the principal to be used solely by the School. Evidence of such contract shall be produced within 2 weeks upon awarding of Contract.

10.6. Technical Design Consideration

Programs

- 10.6.1. The System shall be designed and configured to perform with high performance, maintainability, integrity, reliability, availability, scalability, tight security and control as the primary consideration.

- 10.6.2. The System shall be viewable using, at minimum, major web browser from Microsoft Edge, Google Chrome, Apple Safari, and Mozilla Firefox.
- 10.6.3. As the recommended browsers including their versions change from time to time, the Contractor will need to ensure the compatibility, and ensure the proposed solution is compatible with new browser provider that has gained popularity and to provide a plan to support them in the roadmap.
- 10.6.4. The System should be modular and well designed, so that future enhancements can be easily incorporated. The Contractor shall not create a separate program if same program is used by different user types.
- 10.6.5. There shall be no hard coding of ID(s), Password(s) or any similar parameters in the System. User-defined parameters, look-up tables or system configurable parameters shall be provided as much as possible. As far as possible, the System shall be designed to be parameter driven to allow the System to be flexible to accommodate changes without amendments to program.
- 10.6.6. No hard coding of IP address shall be included into programs. The Contractor shall not implement a solution using IP address to maintain sessions.
- 10.6.7. The System shall be designed such that it can operate in a centralised mode (i.e. serving multiple remote offices via leased line, running off a central hosting farm). In a centralised mode, the System shall allow a centralised Access Control Administrator to maintain user groups / roles.
- 10.6.8. The Contractor shall develop built-in redundancies to prevent single point of failures which can bring down the entire System.
- 10.6.9. The use of Common Gateway Interface (CGI) script is not allowed.
- 10.6.10. Passing parameters in URL is not allowed. The System shall use server-side parameter passing where possible.
- 10.6.11. For web pages generated by the System which contain sensitive data (e.g. user personal data), the System shall employ expiry tags so that such pages are never cached.
- 10.6.12. Configurable timeout and logout features shall be set for non-active sessions.
- 10.6.13. The Contractor shall provide workstation security by using an automatic time-out mechanism and by limiting access to the System through the use of valid user-ids and individual passwords.
- 10.6.14. The System shall allow only single login session for each valid user-id; and concurrent login for same user-id is not allowed.

Client Workstation

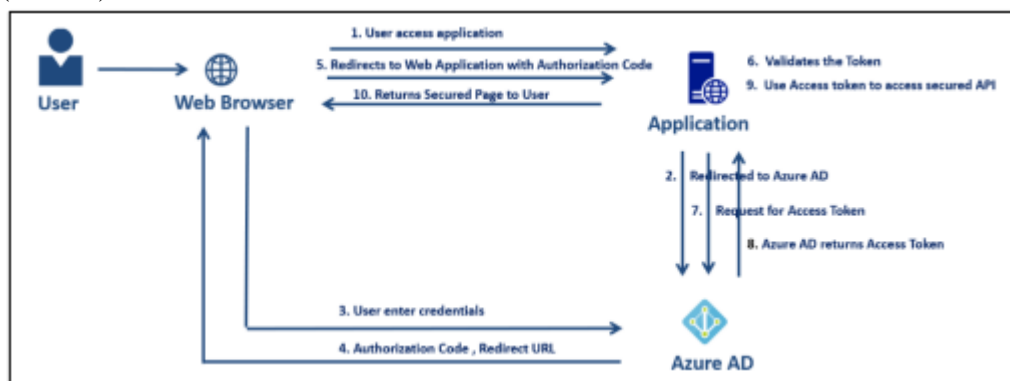
- 10.6.15. All web browser plug-ins required shall not be proprietary in nature, and shall be fully supported locally.
- 10.6.16. The Contractor shall specify clearly in the tender proposal, the list of proposed web browser plug-in, if any, together with the detailed cost in the project cost summary.

10.7. Interface Requirements

- 10.7.1. The System shall integrate with existing SFTP, APIs using standard protocols (such as JWT and REST) to facilitate seamless integration with Schools' applications systems (Asset Management System, Student Information & Administration System) and external agencies/ bank (IRAS, CPF and Banks) when required, if necessary.
- 10.7.2. The Tenderer shall ensure that all data in transit and at rest (if required) is encrypted and secured using industry-standard protocols and best practices. This includes, but not limited to, the use of secure transport layer protocols (such as TLS/SSL) for data transmission over networks.
- 10.7.3. The Tenderer shall implement appropriate measures to protect against unauthorised access, accidental loss, destruction, or damage of data during transmission.

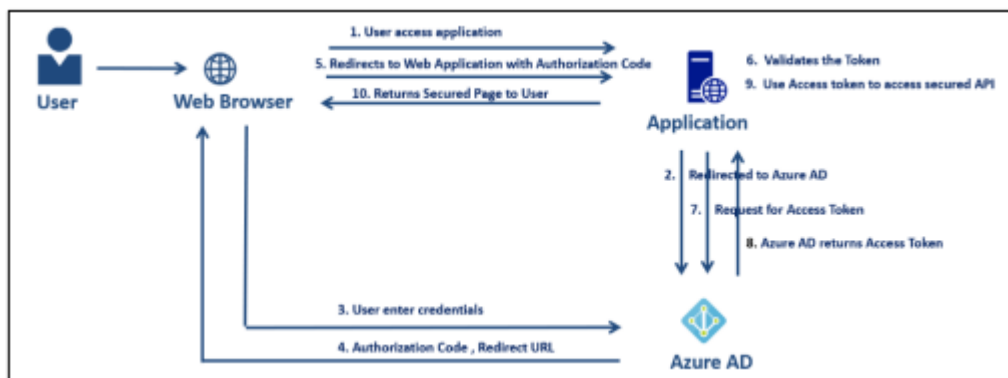
10.7.4. Identity Store

- 10.7.4.1. Azure Active Directory (AAD) is the centralized cloud-based authentication service for intranet and internet applications using school credentials. This section describes details on onboarding of custom developed agency applications using Azure AD. Two authentication standards supported by AAD are OpenID Connect (OIDC) and Security Assertion Markup Language (SAML).

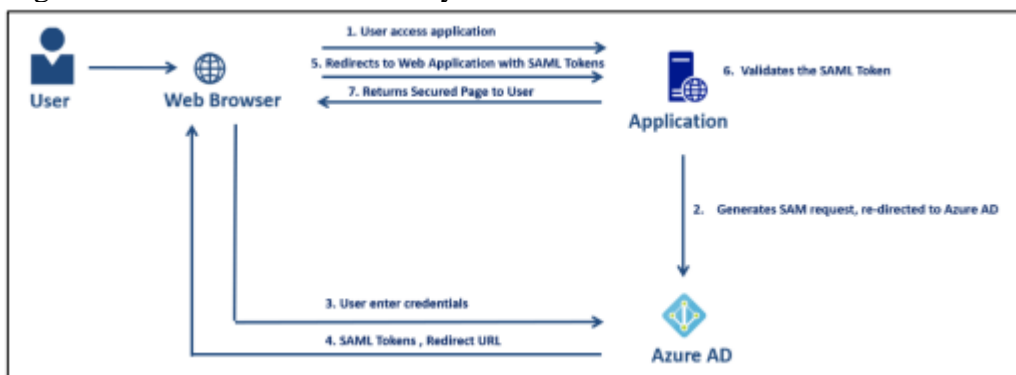


- 10.7.4.2. OpenID Connect is the authentication protocol built on OAuth authorization framework to sign-in users to application. In OIDC authentication flow, user is redirected from browser and user details/attributes are retrieved using Microsoft Graph API. There are different authentication flows available in OIDC for

server-side, mobile, desktop, machine-to-machine applications, more details are available here. Below diagram shows most common OIDC Authorization code flow.



- 10.7.4.3. SAML is XML-based standard used for single sign on implementations. In SAML authentication flow, user is redirected from browser and user details/attributes are available in authentication response. Thus, application hosted network and Azure AD do not need network connectivity to communicate and the browser acts as a middleman to communicate. Below diagram shows the most commonly used flow in SAML based on redirection.



- 10.7.4.4. Application authentication protocol should be decided based on cloud service provider and use case. OIDC is preferable due to lightweight, API/REST based architecture, support for mobile and single page applications. SAML is heavy weight due to size of XML message transmitted

11. INTENTIONALLY LEFT BLANK

12. SECURITY REQUIREMENTS

12.1. General Security Requirements

- 12.1.1. The Contractor shall ensure that all security requirements under this section, regardless of the sub-section it is located, are applied to the entire scope of this Contract unless otherwise stated. Where the School has exercised the option within the Contract, the Contractor shall ensure that all applicable measures set out in this document are implemented.
- 12.1.2. INTENTIONALLY LEFT BLANK.
- 12.1.3. The Contractor shall ensure data and information is protected from leakage, loss, destruction and falsification in accordance with statutory, regulatory, contractual and business requirements. The Contractor shall protect the data and information regardless of the format in which they are held in.
- 12.1.4. The Contractor shall incorporate the following security principles in the design, implementation and operations of the System:
- (a) Confidentiality (non-disclosure of information to unauthorised entities);
 - (b) Integrity (substantiate the accuracy and completeness of the information);
 - (c) Availability (accessible and usable when authorised entities require access);
 - (d) Compliance (conformance to established policies, regulations and standards); and
 - (e) Access control (manage and control access to resource by authorised entities).
- 12.1.5. The Contractor shall fully comply with any written instructions on ICT security related matters that are issued by the Government and the School from time to time.
- 12.1.6. The Contractor shall provide technical advice on the network, system, database and applications when requested during security risk analysis, security standards and policy implementation specific to the System.
- 12.1.7. The Contractor shall ensure that all security procedures within their area of responsibility are implemented correctly to achieve compliance with relevant security policies and standards.
- 12.1.8. The Tenderer shall declare all security limitations relating to the security design and implementation for System.

12.1.9. The Contractor shall ensure that unless otherwise stated explicitly, all additional resources and manpower provided to resolve IT security related issues under the responsibilities of the Contractor, such as rectifying vulnerabilities and mitigating risks, shall not incur additional cost to the School.

12.1.10. The Tenderer shall state any security-related certifications they have attained, such as ISO/IEC 27001 or ISO/IEC 27018, and CSA STAR or Information Technology Infrastructure Library (ITIL) v3, for security management, governance framework and operations.

12.2. Assets Management

12.2.1. The Contractor shall develop and maintain an inventory of all materials and assets relevant to this Contract, and update the School within ONE (1) month upon a change in the inventory.

12.2.2. The Contractor shall ensure the School's assets and/or information shall be protected from loss, leakage, destruction, unauthorised modification, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

12.2.3. The Contractor shall report any loss of the School's assets and/or information immediately in accordance with the School's security incident response plan.

12.3. Information Classification and Handling

12.3.1. The Contractor shall observe the secure usage and handling of all data/information in accordance to their classifications.

12.3.2. The Contractor shall be accountable to protect all information related to the System entrusted to them to ensure that it is not used for other purposes unless the use is authorised by the School. The Contractor shall be responsible for the safeguarding of security-classified information under their care.

12.3.3. The Contractor's personnel shall sign confidentiality agreements prescribed by the School to ensure no unauthorized disclosures of security-classified or sensitive information received or generated under this Tender or Contract unless specifically authorized by the School in writing. The Contractor shall ensure that all its personnel and Subcontractors are informed that failure to comply with this agreement would be a criminal offence and may lead to persecution.

12.3.4. The Contractor shall not disclose security-classified information received or generated under this Contract or Tender to unauthorised personnel unless specifically authorised in writing by the School. This includes the source of the information. In addition, the Contractor shall ensure that discussions on the information shall be conducted in secured areas where it is not subjected to disclosure to unauthorised personnel. For example, the Contractor must not conduct discussions on classified matter (e.g. system design and architecture) in public areas such as cafes and restaurants.

- 12.3.5. The Contractor shall ensure that all security classified information in its portable computers and external storage devices, such as flash drives, are stored in an encrypted form using desktop security software authorized by the School. Portable computers unable to support such designated desktop security software shall not be used to store or transmit any security classified information. The Contractor shall also bear the costs involved with the use of the designated desktop security software.
- 12.3.6. The Contractor shall not transfer security-classified information or personal data held in connection with this Contract outside Singapore, or allow parties outside Singapore to have access to it, without prior approval in writing by the School.
- 12.3.7. Upon completion of the Contract, the Contractor shall return all security classified materials received or generated under this Contract (including approved photocopied materials) and perform secure erasure/destruction of security classified data. The tools and procedures for secure erasure / destruction shall be subjected to approval by the School.
- 12.3.8. The Contractor shall not publicly disclose information even if information has been declassified. The Contractor shall request for approval for public disclosure of such declassified information from the School.
- 12.3.9. The Contractor shall ensure that its personnel and Subcontractor do not keep any security-classified information upon departure from his/her appointment or retain such information when he / she no longer requires them.
- 12.3.10. The Contractor shall define and implement procedures to ensure that all data and information stored in the System are securely erased when they are no longer required such that the stored data and information cannot be recovered. The tools and procedures for secure erasure/destruction shall be subjected to approval of the School.
- 12.3.11. The Contractor shall immediately notify the School when it becomes aware of a disclosure or leakage of any security-classified or sensitive information acquired in connection with this Contract.
- 12.3.12. The Contractor, its employees, agents, and Subcontractors shall not disclose information from the Contract upon termination or expiration of this Contract.
- 12.3.13. In the event Contractor need to send information (e.g. logs for troubleshooting) to third party, sensitive information such as Internet-Protocol (IP) address, hostname, user ID must be sanitised prior to sending it out. The sanitised information shall be subjected to approval of the School before sending to the third party.
- 12.3.14. The Contractor shall ensure that all classified or sensitive data in-transit and at-rest (including backup and archived data) within the System are encrypted with approved cryptographic algorithms. (Details in Section 12.17 - Cryptography)

12.4. Personnel Requirements

- 12.4.1. The Contractor shall observe the secure usage and handling of all the School's information.
- 12.4.2. The Contractor shall subject all their personnel who will be involved in the System to security clearance by the School before commencing their work.
- 12.4.3. The Contractor shall ensure that all the Contractor's personnel's security clearance commensurate with the highest security classification of information that he/she has been given access to. In addition, the Contractor's personnel shall only be granted access to information that is relevant to the discharge of his/her duty.
- 12.4.4. The School reserves the right at any time to reject any of the Contractor's personnel and the Contractor is responsible to find replacements immediately and at the Contractor's own expense.
- 12.4.5. The Contractor shall define and communicate the roles and responsibilities to all personnel involved in the project in accordance with the requirements of this Contract. The defined roles and responsibilities shall consider the need for separation of duties to avoid potential for conflict of interests and the level of authorisation accorded to the roles. The Contractor shall provide detailed description of the roles and responsibilities vis-à-vis the list of personnel who will be involved in the project.
- 12.4.6. The Contractor shall conduct appropriate background checks on all its personnel involved in this project.
- 12.4.7. The Contractor personnel who will be assigned to perform the required security services under this Contract shall already be trained and possess the relevant technical expertise and experience to carry out the security services.

12.5. Security Risk Management

- 12.5.1. The Contractor shall implement the security risk management processes, standards and procedures for the System and demonstrate conformity via deliverables such as audit reports or security testing reports. The security risk management process shall align with the School's risk management methodology.
- 12.5.2. The Contractor shall implement appropriate control strategies that are consistent with the School's security policies and standards to mitigate the identified risks, threats and vulnerabilities.
- 12.5.3. The Tenderer shall provide a detailed description of the risk management process and how it will be applied to the System. The risk management process shall minimally include the following:
- (a) Risk identification;

- (b) Risk assessment;
 - (c) Risk response;
 - (d) Risk control activities; and
 - (e) Risk monitoring and review.
- 12.5.4. The Contractor shall perform regular ICT security risk assessments for the System together with the School according to the School's risk management methodology, and maintain an updated security risk register for the duration of the Contract. The ICT security risk register, as well as its subsequent updates and changes shall be subjected to review and approval of the School.
- 12.5.5. The Contractor shall review ICT security risks for the System together with the School, when instructed by the School or whenever there is any major change. Examples of major change are:
 - (a) Impacts the security function of the application system (such as authentication, access controls, logging, etc.); or
 - (b) Has high or medium business impact to the application system (such as those affecting key business functions).
- 12.5.6. The Contractor shall submit the ICT security risk assessment report to the School within TEN (10) working days upon the completion of each security risk assessment.
- 12.5.7. The Contractor shall propose alternative controls to address or mitigate the risks to a level that is acceptable to the School.
- 12.5.8. The Contractor shall propose response and recovery plans for each corresponding risk identified in the event a risk materialises despite the security mitigations put in place.
- 12.5.9. The Contractor shall ensure that the risk register is updated with the latest security risk information including inputs from the security assessments performed by the independent security assessors. The risk register shall be provided to the School upon request.
- 12.5.10. The Contractor shall have clearly defined roles for all information security responsibilities in accordance with the System's security policy. The information security roles shall consider the need for segregation of duties required of each role and the level of authorisation accorded to the roles.

12.6. Security Monitoring

- 12.6.1. The Contractor shall implement security monitoring mechanisms to monitor all security-related events for timely detection of suspicious events or malicious activities and alerts shall be triggered to relevant personnel when such events or activities are detected.
- 12.6.2. The Contractor shall ensure the security monitoring rules defined, implemented and maintained are relevant and specific to the System, and the School shall reserve the rights to provide inputs and change security monitoring rules at no charge to the School.
- 12.6.3. The Contractor shall provide the tools/utilities to detect, log and alert any illegal changes to the System website in real-time, and ensure that a correct version is automatically restored within FIVE (5) minutes if unauthorised changes have occurred.
- 12.6.4. The Contractor shall make available all required logs for security monitoring. Examples of sources of such logs are:
- (a) Operating Systems;
 - (b) Databases;
 - (c) Applications;
 - (d) Network intrusion Detection and Prevent Solutions (NIDPS);
 - (e) Anti-malware solutions;
 - (f) Firewalls;
 - (g) Authentication and authorisation services;
 - (h) Remote access solutions;
 - (i) Web proxies;
 - (j) Domain Name Services (DNS);
 - (k) Dynamic Host Configuration Protocol (DHCP) Service.

12.7. Security Testing

- 12.7.1. The Contractor shall reference the latest industry security standards and best practices for security testing such as:
- (a) Center for Internet Security (CIS) Benchmarks;
 - (b) Open Source Security Testing Methodology Manual (OSSTMM);

- (c) Open Web Application Security Project (OWASP) Testing Guide;
 - (d) OWASP Mobile Security Testing Guide;
 - (e) Other application security best practices.
- 12.7.2. If scripts and/or programs are used as part of the security testing, the Contractor shall ensure that these scripts and/or programs shall not cause any disruption or damage to the System.
- 12.7.3. For all Security testing activities, the Contractor shall propose an appropriate test plan, subjected to approval by the School. The plan should include:
 - (a) Test scope;
 - (b) Objective of each test;
 - (c) Assumptions and limitations (if any);
 - (d) Detailed test cases (i.e. including test scenario / setup, detailed steps to perform the test, tools to be used, required inputs, expected outputs/results, actual outputs/results, etc.);
 - (e) Designated Contractor personnel expected to be performing the tests;
 - (f) Other personnel expected to be involved (i.e. supporting or assisting) in the test;
 - (g) Schedule to perform the test and follow-up action (if any);
 - (h) Test environment;
 - (i) Test asset; and
 - (j) Reporting format.
- 12.7.4. The Contractor shall analyse the risk and assign a risk rating (Critical, High, Medium, Low) for each identified vulnerability. The results shall be documented and should include the following:
 - (a) Findings and observations;
 - (b) Risk rating;
 - (c) Implications;
 - (d) Recommendations (by independent security consultant); and
 - (e) Remediation status (applicable to follow up testing).

12.7.5. The Contractor shall ensure that all known IT security vulnerabilities are addressed.

1.1.1 The Contractor shall work with the School to conduct the following security testing activities prior to System commissioning or when System undergo changes that impact security controls or have high impact to business functions, where applicable:

- a. Source code review / scanning; and
- b. IT Security review (i.e. compliance, configuration, technical architecture);

Pre-Commission

12.7.6. The Contractor shall work with the School to conduct the following security testing activities prior to System commissioning or when System undergo changes that impact security controls or have high impact to business functions, where applicable:

- (a) Source code review / scanning; and
- (b) IT Security review (i.e. compliance, configuration, technical architecture);

Source Code Review

12.7.7. The Contractor shall ensure code review cover all parts of the application so that the application does not have erroneous, hidden or malicious code before deployment to production.

12.7.8. If source code review cannot be performed due to the lack of access to application source code (i.e. commercial off the shelf software, software as a service and etc.), the Contractor shall provide security assurance that the application is written correctly, implements the desired design, and does not violate any security requirements. Examples of security assurance: 3rd party security testing of the source code or equivalent, as well as evidence of secure development lifecycle during the development of the application.

12.8. ICT and Data Security Incident Management

- 12.8.1. The Contractor shall develop, implement and maintain an ICT and Data Incident Management Plan and handling procedures for the System together with the School. The Contractor shall ensure that the developed ICT and Data Incident Management Plan and its subsequent updates are subjected to approval of the School. The ICT and Data Incident Management Plan shall minimally include the following:
- (a) Pre-incident preparation including incident management planning, awareness and education as well as training and exercises;
 - (b) Detection and analysis including scenarios, thresholds and procedures for activation of incident reporting and response;
 - (c) Response and remediation including impact containment, service and system recovery, investigation and forensics, and evidence preservation including log and equipment acquisition, seizure of evidence and placement of monitoring equipment where applicable; and
 - (d) Post-recovery inquiry including post-incident reviews and recommended mitigating actions to prevent a recurrence.
- 12.8.2. The Contractor shall ensure that all their personnel involved in the System are briefed on the incident handling procedures.
- 12.8.3. All suspected or confirmed incidents, e.g. virus infection, system or data compromises, unauthorised access, data exposure, etc. shall be reported to the School immediately. The Contractor shall take the necessary actions to ensure that all system and data incidents are reported, handled and managed in accordance to the timeframe agreed with the School.
- 12.8.4. In the event of any ICT system or data security incidents, the Contractor's responsibilities shall include:
- (a) Impact containment, service and system recovery, investigation and forensics, and evidence preservation including log and equipment acquisition, seizure of evidence and placement of monitoring equipment where applicable;
 - (b) Ensuring the preservation and admissibility of evidence by protecting and documenting all access to incident information; and
 - (c) Exercising the prescribed incident response guidelines and procedures of the ICT and Data Incident Management plan of the System.
- 12.8.5. The Contractor shall generate detail incident report for each system or data incident and submit it to the School. The format of the incident report shall be subjected to the approval of the School.

- 12.8.6. The Contractor shall implement measures to prevent the recurrence of system or data incidents.
- 12.8.7. The Contractor shall work with the School in resolving system and data incidents by activating appropriate personnel and resources for investigation and resolution purposes.
- 12.8.8. The Contractor shall notify the School and the School designated representative within the specified time upon detection of incident. The Contractor shall adhere to the response time and frequencies stated in the following table:

Incident Severity Classification	Timeframe for Follow-on Reports			Resolution Time
	Verbal Report	Incident Report Form	Status Update	
High	Within FIFTEEN (15) minutes upon detection of suspected or confirmed incident	Within TWELVE (12) hours upon detection of suspected or confirmed incident	Every TWO (2) hours until normal operations have resumed or as directed by the School	Resolve within 1 hour of problem occurrence - otherwise implement workaround within 2 hours
Medium	Within TWO (2) hours upon detection of suspected or confirmed incident	Within TWENTY-FOUR (24) hours upon detection of suspected or confirmed incident	Every TWELVE (12) hours until normal operations have resumed or as directed by the School	Resolve within 4 hours of problem occurrence - otherwise implement workaround within 6 hours

Low	Contractors shall maintain an internal record of these incidents based on the above information gathered and submit this record to the School on a monthly basis for review and verification of the impact assessment or when the record is requested by the School	Resolve within 6 hours of problem occurrence - otherwise implement workaround within 8 hours
-----	---	--

12.8.9. The Contractor shall note that the incident severity classification level of a system or data incident may be escalated or reduced over time. For example, an incident that is classified as “Medium” may be escalated to “High” if the seriousness or impact is bigger than initially determined.

12.8.10. The Contractor shall perform root cause analysis on all incidents. The School, however, reserves the right to undertake parallel investigations or take over any ongoing investigations that it deems as critical. The Contractor shall ensure that tools used in the root cause analysis are able to preserve evidence for admission in court.

12.8.11. The Contractor shall also compile a monthly report summarising all system and data incidents that occur within the month and submit it to the School.

12.9. Security Training and Awareness

12.9.1. The Contractor shall ensure that all personnel are equipped with the relevant knowledge, skillsets and experience to implement and maintain the System in a secure manner. The personnel shall be familiar with the security requirements of the System and shall adhere to the security policy, standards and procedures as approved by the School.

12.9.2. The Contractor shall ensure that all their personnel involved in the System are informed of their security responsibilities and accountabilities/liabilities before putting the person in his/her assigned areas of work. The Contractor shall also ensure that their personnel (including Subcontractors) are briefed on established security policies, rules and procedures pertaining to working with the School designated hosting environment and the School-appointed Contractors. The briefing shall minimally include:

- (a) IT security threats and protection mechanisms;

- (b) Security policies, standards, processes and procedures required for their work;
- (c) Information handling requirements;
- (d) Process for reporting issues that may lead to an IT security incident; and
- (e) Security incident root cause analysis, case studies, reflection on past incidents.

12.9.3. The Contractor shall be responsible for the security education and training of their personnel (including Subcontractors) and formulate a learning roadmap to meet the needs, especially for new recruits and those taking on new posts and duties for this Contract and whenever there is significant change to the usage of the System. The Contractor shall ensure security training is conducted for all its staff and keep records of all staff who have successfully completed the training.

12.10. Business Continuity Management

12.10.1. The Contractor shall work with the School to develop and document business continuity framework for the system / service, and plan to ensure core business operations can continue when disruptive events occur. The plan shall minimally include:

- (a) Security considerations;
- (b) Emergency response;
- (c) Incident response;
- (d) Recovery procedure; and

12.11. System Security

12.11.1. The Tenderer shall propose a detailed system design in its Tender Offer, which shall at least include the network and security architecture, components, interfaces, protocols, security controls, as well as management and administration mechanisms.

12.11.2. The Contractor shall develop and maintain the security architecture or design of the System together with the School. The security architecture and its subsequent updates shall be subjected to the approval of the School.

- 12.11.3. The Contractor shall develop, implement and maintain security configuration guides, hardening guides and baselines for the System to ensure configurations are secure, for all parts of the System, including Operating Systems, applications, and databases, subjected to the School's approval. The Contractor shall take reference from security configuration guides published by Center for Internet Security (CIS) or equivalent security standard body, and product principals. The Contractor shall also review and update the security configuration guides annually or whenever informed by the School. If the relevant guides and baselines do not exist, the Contractor shall provide information on how the systems can be secured to a level that is acceptable to the School.
- 12.11.4. The Contractor shall establish a system-hardening framework that governs the processes of hardening all systems, Basic Input-Output System (BIOS) and applications. The established framework shall be clearly documented in a "System Hardening Framework Document" and provided to the School for approval within the timeline determined by the School. The Framework document shall be maintained, review and updated by the Contractor annually, subjected to the School approval. The Framework document shall minimally include:
- (a) Methodology and process of creating the system hardening checklists and whether the checklists are based on industry standard hardening baselines such as CIS, or equivalent;
 - (b) Process to implement the hardening checklists and how all items stated in the hardening checklists can be verified to be correctly implemented on each system; and
 - (c) Roles and responsibilities of various parties that are involved in the system hardening and verification process;
- 12.11.5. The Contractor shall implement a mechanism to track the expiry dates of all digital certificates to ensure timely renewal of expiring certificates. The mechanism is subjected to approval by the School.
- 12.11.6. If any digital certificates expire at any time during the Contract Period, the Contractor shall inform the School TWO (2) months before expiry or mutually agreed timeline and ensure timely renewal of expiring digital certificates.
- 12.11.7. The Contractor shall not use Contractor-supplied external media such as hard disk or thumb drives. Where instructed by the School to use Contractor-supplied external media, the Contractor shall ensure that these external media are free of malicious content before using.
- 12.11.8. The Contractor shall ensure all test data, test accounts, and test credentials are removed from production system before the system commissioning.
- 12.11.9. The Contractor shall run applications and batch jobs using accounts with the least privileges unless otherwise approved by the School.

- 12.11.10. The Contractor shall ensure that adequate security measures are taken throughout the entire lifecycle of the System to meet the security requirements for the System.
- 12.11.11. The Contractor shall periodically review and identify any possible security risks and threats pertaining to the design of the System. Based on the risks and threats identified, the Contractor shall propose and implement mitigation measures, subjected to the School approval.
- 12.11.12. The Contractor shall ensure that all part of the System, including IT assets and tools used in relation to the System is not end-of-support (EOS). Should any part of the System reach EOS, the Contractor shall propose and implement alternative solutions while still maintaining compliance with this Contract, at no additional cost to the School.
- 12.11.13. The Tenderer shall propose Common Criteria (CC) certified products, whenever feasible. For products that are CC certified, the Tenderer shall indicate the conformance to Collaborative Protection Profile (CPP) or Evaluation Assurance Level (EAL). For products that are in the midst of CC certification, the Tenderer shall elaborate on the schedule of activities and relevant protection profiles for CC certification.
- 12.11.14. The Contractor shall implement anti-virus or anti-malware software in the System across all environment (i.e. User Acceptance Testing (UAT), development and production environment) to prevent, detect (on-access and on-demand) and remove malicious codes from systems or devices, files and embedded objects in files, and ensure that the solution meets the following:
- (a) For systems or devices with NAC, the definition file shall not be more than seven calendar days old; or
 - (b) For systems or devices not governed by NAC, the anti-virus or anti-malware solution in the System are updated daily with patches and signatures from approved sources.
- 12.11.15. The Contractor shall work with the School-appointed Contractors to ensure that any malware detected by the anti-malware solution is removed from the System across all environments (i.e. UAT, development and production environments) immediately, and the appropriate security event logs generated to record the detection and removal of the malware. The Contractor shall also ensure that personnel designated by the School is alerted of all security incidents.
- 12.11.16. The Contractor shall work with the School-appointed Contractors to ensure full system malware scans throughout the System is performed periodically, and immediately report to the School any findings from such scans. The frequency of the scan shall be specified by the School.
- 12.11.17. The Tenderer shall develop and maintain a security guidelines document covering the scope of the System based on minimally:

- (a) System and data confidentiality, integrity and availability;
 - (b) Data privacy;
 - (c) Data handling; and
 - (d) Secure coding procedures in the language chosen for the application.
- 12.11.18. The Contractor shall review and update the content of the security guidelines document, subjected to approval by the School.
- 12.11.19. The Contractor shall implement a secure workflow to ensure there is a process and security mechanism (e.g. content filters) to filter, review and approve the content contributed by or aggregated from multiple parties, prior to publication on the web-site. The Tenderer shall in its proposal describe how this is achieved.
- 12.11.20. The Contractor shall ensure that any web-authoring functionality, e.g. via WebDAV-based features, is made available to authenticated, approved users only.
- 12.11.21. The Contractor shall ensure that content aggregation, e.g. RSS syndication and via portlets, is done securely, where contents aggregated into the System are retrieved from trusted sources only.
- 12.11.22. The Contractor shall ensure that where a web source offers HTTPS access, the System will use HTTPS for retrieving and transporting data.
- 12.11.23. The Contractor shall ensure that all remote file transfers to / from / within the System are performed using SSH File Transfer Protocol (SFTP) or other secured file transfer mechanisms subjected to approval by the School.
- 12.11.24. The Contractor shall ensure that all administration modules of the System are accessible only from pre-identified network addresses.
- 12.11.25. The Contractor shall ensure all classified sections of the System are protected by authentication and proper access control.
- 12.11.26. The Contractor shall ensure security penetration testing is carried out on the System in the following categories:
- (a) New systems that have yet to be deployed into production environments;
 - (b) Changes to existing system that impact security controls or business functions; and
 - (c) Periodic test on existing system. The frequency shall be determined and updated by the School.
- 12.11.27. The security penetration test plans shall be subjected to approval by the School before conducting the test.
-

- 12.11.28. The Contractor shall ensure access to the database is performed by authorised personnel only. All activities on the database by these personnel shall be logged and monitored.
- 12.11.29. The Contractor should ensure that all queries and actions (e.g. insert, update, delete) to database(s) in the System are performed through secure programmatic methods (e.g. stored procedures).
- 12.11.30. The Contractor shall ensure proper measures are built into the application to improve security and robustness for each end-user queries and actions. These measures shall at least include the following:
- (i) Enforce the type of query parameters; and
 - (ii) Limit the volume of records returned from user'' queries in a single query instead of providing a data dump.
- 12.11.31. The Contractor shall ensure that application/service accounts for accessing the database, are not used by any individual users to login to the System.
- 12.11.32. The Contractor shall not use production environments for testing or development or use production data (unless production data has been desensitised) in a non-production environment.
- 12.11.33. The Contractor shall not use production Uniform Resource Locator (URL) and secrets (e.g. passwords, API keys, cryptographic keys) in non-production environment.
- 12.11.34. The Contractor shall ensure the System have proper authentication (e.g. API Keys) and secure channel for access (e.g. TLS) to all exposed APIs.
- 12.11.35. The Contractor shall ensure the System have proper validation of all API requests.
- 12.12. Network Security**
- 12.12.1. The Tenderer shall provide a description of the network, which shall at least include the architecture and design, the protocols, the System and their interfaces, the security features, the technologies and solutions, the administration and usage processes and procedures.
- 12.12.2. The Contractor shall implement the following security design practices into the System:
- (a) Deny network traffic by default;

- (b) Isolate the internal network segments from the external network (e.g. Internet, other networks not part of this System) and other geographically separate sites through appropriate access controls such as firewalls (network-layer and application-layer), proxy servers or application security gateways. Where possible, all incoming and outgoing traffic shall be subjected to filtering and inspection;
- (c) Use network-based and/or application firewalls for the perimeter, and ensure network perimeter firewalls does not provide unrelated and non-security application services;
- (d) Ensure web proxy server implements authentication mechanism for web access validation and tracking, implements content filtering with reputation-based filtering for URLs (and URL blacklisting, if possible), implements signature-based/heuristic-based scanning, detection and blocking of all malicious files and web objects, and filters malicious file types (e.g. executable files);
- (e) Implement separate environments for the system development, testing and production;
- (f) Implement strict network access controls (NAC) to restrict remote administrative access to selected network addresses;
- (g) Use non-default network ports for access to remote administration features;
- (h) Implement authentication, authorisation, or payload inspection for all incoming connections;
- (i) Implement network-based firewalls to block both unauthorised inbound and outbound network traffic;
- (j) Implement host-based firewalls to protect endpoint devices against unauthorised network connections, where possible; and
- (k) Implement application firewalls to filter unauthorised application and service requests, whenever required.

12.12.3. The Contractor shall ensure that threshold limits and other appropriate security mechanisms are implemented at the network perimeter gateways to mitigate against Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.

12.12.4. The Contractor shall ensure network intrusion detection systems (NIDS) / Network intrusion Prevention Systems (NIPS) are implemented at the following logical locations:

- (a) For systems directly accessible from the Internet, NIDS / NIPS shall be implemented before Internet traffic reaches the outermost firewall;

- (b) For systems such as directory servers and DHCP servers, NIDS / NIPS shall be implemented before network traffic reaches the nearest firewall; and
 - (c) The management interface of the NIDS/NIPS shall not be directly connected to the Internet and the management traffic shall not traverse to the Internet.
- 12.12.5. The Contractor shall propose a NIDS/NIPS that minimally support the following features to detect unknown network attacks and/or anomalies:
 - (a) Signature-based detection;
 - (b) Anomaly-based detection;
 - (c) Frequency / threshold detection;
 - (d) Stateful protocol analysis;
 - (e) Whitelisting of permitted traffic;
 - (f) Blacklisting of denied traffic;
 - (g) In-line deployment; and
 - (h) User-defined signatures.
- 12.12.6. The Contractor shall ensure the proposed NIDS/NIPS shall provide alert mechanisms in response to critical events. The alert mechanisms shall support the following:
 - (a) SNMP v3 and higher;
 - (b) Console alerts; and
 - (c) Internet SMTP;
- 12.12.7. The Contractor shall ensure that there is no network connection to any external network, e.g. modem dial-up connection that bypass the controls enforced at the central gateway.
- 12.12.8. The Tenderer shall submit proposal of, unless there is good reason, a System design based on a multi-tier architecture that differentiates major functions and components like presentation tier, application tier and data-tier to segregate input/output screens, business and interface logic, and functions related to the processing of data. The Contractor shall implement the proposed design subjected to the agreement of the School.

- 12.12.9. The Contractor shall ensure all inter-system communication (i.e. communication with an external system) channels (the transmission of all transactions and data traffic with external networks) shall be protected using channel encryption and authentication.
- 12.12.10. The Contractor shall ensure all intra-system (e.g. server-to-server, client-to-server.) communication channels shall be protected using channel encryption (i.e. communication channel encryption must not be broken between source to destination machine).
- 12.12.11. The Contractor shall implement appropriate security measures to ensure that transport level security measures (for example TLS, etc.) are implemented subjected to approval by the School. The measures shall minimally cover the following:
- (a) Enable at least TLS 1.2;
 - (b) Set the secure flag on all sensitive cookies;
 - (c) Set the HttpOnly flag on all sensitive cookies;
 - (d) Use only approved cipher suites as defined in Section 18;
 - (e) Use valid digital certificates; and
 - (f) Encrypt backend connections.
- 12.12.12. The Contractor shall ensure the proposed System have an encryption scheme to protect classified and/or sensitive on storage components (such as database) of the System from unauthorised access, modification and destruction.
- 12.12.13. The Contractor shall ensure all proposed servers in the System support policy configuration over secured communications channels from authorised management system.
- 12.12.14. The Contractor shall ensure all administration and management access can only be accessible from authorised network addresses and workstations.

12.13. Application Security

- 12.13.1. The Contractor shall ensure that security is built into each stage of the Software Development Life Cycle (SDLC). The Contractor shall implement industry standards or framework, such as Open Web Application Security Project (OWASP) Application Security Verification Standard (ASVS) to meet this objective. The Contractor shall identify security weaknesses, propose mitigation and improvement measures for review with the School.

- 12.13.2. The Contractor shall make use of code scanning service provided by the School-appointed Contractors to identify common vulnerabilities as part of the SDLC, and ensure identified vulnerabilities are remediated before deploying to Production environment. The Contractor shall furnish the code scanning result and remediation status for approval by the School before deploying to Production environment.
- 12.13.3. The Contractor shall incorporate security requirements into the SDLC with activities such as threat modelling, scanning using automated testing tools for common vulnerabilities and security code reviews. The Contractor shall share details of the activities carried out, counter-measures or fixes used, tools used in the testing and the findings with the School.
- 12.13.4. The Tenderer shall submit a security risk profile for all proposed commercially off-the-shelf (COTS) software. The security risk profile should contain any security vulnerability or weakness pertaining to the COTS software. The Contractor shall also propose mitigation measures or workarounds to address the identified vulnerability or weakness, subjected to approval by the School.
- 12.13.5. The Contractor shall use security control libraries such as OWASP's Enterprise Security API (ESAPI) for the programming languages used in the System, which can help enforce application wide security practices, and additional validation measures instead of individual page-based measures to provide a consistent level of security across the application.
- 12.13.6. The Contractor shall ensure that the application is not affected by at least the following vulnerabilities:
- (a) Injection;
 - (b) Broken Authentication;
 - (c) Sensitive Data Exposure;
 - (d) XML External Entities (XXE);
 - (e) Broken Access Control;
 - (f) Security Misconfiguration;
 - (g) Cross-Site Scripting;
 - (h) Insecure Deserialization;
 - (i) Using Components with Known Vulnerabilities;
 - (j) Insufficient Logging & Monitoring.
 - (k) Cross Site Scripting (XSS);
 - (l) Broken Session Management;

- (m) Insecure Direct Object References;
- (n) Cross Site Request Forgery (CSRF);
- (o) Insecure Cryptographic Storage;
- (p) Failure to Restrict URL access;
- (q) Insufficient Transport Layer Protection;
- (r) Unvalidated Redirects and Forwards;
- (s) Buffer overflows; and
- (t) Improper error handling.

12.13.7. The Contractor shall implement input validation for all data that is received and processed by an application. The input validation shall be performed at the server end, and where applicable at the client end. The validation shall minimally cover the following:

- (a) Usage of positive input validation (i.e. accept what is allowed only);
- (b) Type validation (e.g. numbers should not include alphabets or special characters);
- (c) Length validation (e.g. minimum number of characters, maximum number of characters);
- (d) Syntax validation and null validation;
- (e) Escaping of special characters, if parameterized APIs are not available; and
- (f) Escaping of all untrusted data in HTML contexts.

12.13.8. The Contractor shall reference the latest Open Web Application Security Project (OWASP) Top 10 security risks as well as other emerging risks not covered by the OWASP Top 10, and implement mitigation measures against these risks.

12.13.9. The Contractor shall implement appropriate application exception handling mechanisms to display error messages, which does not provide any sensitive information (e.g. stack traces with details of the source code) in the event of any exception in the application.

12.13.10. The Contractor shall implement appropriate session management for application subjected to approval by the School. The implementation shall minimally cover:

- (a) Configurable session timeout periods (THIRTY (30) minutes or as determined by the School);

- (b) Secure transmission of session ID; and
 - (c) Session ID in the cookie instead of URL.
- 12.13.11. The Contractor shall implement appropriate measures to protect sensitive information or functionality with strong access control mechanisms to ensure users accessing different levels of the application are properly authorized. The application shall minimally include the following:
 - (a) Check access control permissions, whenever performing direct object references;
 - (b) Disable directory browsing;
 - (c) Authentication and authorization for each private page;
 - (d) Use of role-based authentication and authorization; and
 - (e) Deny all access by default.
- 12.13.12. The Contractor shall ensure code-review sessions are carried out to ensure that there is no erroneous, hidden or malicious code in the application before deployment to production.
- 12.13.13. The Contractor shall plan and perform System Security Acceptance Test (SSAT), and ensure it is carried out on all application systems, including mobile application (if applicable). The SSAT plan and results shall be signed off when completed.
- 12.14. Access Control**
- 12.14.1. The Contractor shall implement strong authentication and access control mechanisms to ensure that only authorised users are granted access to controlled features of the System, subjected to approval of the School.
- 12.14.2. The Contractor shall ensure that access rights are granted based on principle of least privilege, on job needs, and there are proper procedures for handover and transferring user access credentials due to personnel movement, subjected to approval of the School.
- 12.14.3. The Contractor shall ensure all roles and responsibilities for this System are clearly defined, distinct, there is segregation of roles, and documented, subjected to approval by the School.

- 12.14.4. The Contractor shall review the access rights on regular basis for this System to ensure 21 privileges granted are still appropriate for the corresponding roles and responsibilities. The Contractor shall implement measures to ensure that redundant user accounts and access rights are disabled when they are not used for NINETY (90) calendar days, and removed from the System within FIVE (5) working days upon review and confirmation. Where applicable, automated tools shall be implemented to perform this.
- 12.14.5. The Contractor shall ensure that all accounts (i.e. administrative, system or user accounts) are assigned to individual, who shall be accountable for all actions performed under their assigned account. The Contractor shall ensure that accounts are not shared for accountability reason.
- 12.14.6. The Contractor shall develop, enforce and maintain an access control policy specific to the System. The Contractor shall also review and update the access control policy periodically or whenever necessary, subjected to the approval of the School.
- 12.14.7. The Contractor shall ensure that management consoles or devices for managing the System are dedicated for administration only and not used for any other purpose (e.g. surfing Internet, access email).
- 12.14.8. The Contractor shall have proper approval process and tracking mechanism for all access to the System and information to ensure proper usage and accountability.
- 12.14.9. The Contractor shall develop, enforce and maintain an account management process specific to the System. The Contractor shall also review and update the account management process periodically and whenever necessary, subjected to approval by the School.
- 12.14.10. The Contractor shall implement role-based access control mechanism with sufficient granularity and flexibility that enforces controlled access to all part of the System.
- 12.14.11. The Contractor shall develop, implement and maintain an access control matrix for the System. The Contractor shall also review and update the access control matrix periodically and whenever necessary, subjected to approval by the School.
- 12.14.12. The Contractor shall ensure that there is clear separation of duties for privileged roles in the System such as system, database and application administrators.
- 12.14.13. The Contractor shall ensure that the System allow single user logon session only, such that users (including privileged user) cannot logon to multiple (i.e. concurrent) sessions at any given time using the same user credentials. The Tenderer and Contractor shall highlight any part of the System that cannot enforce single user logon session, and propose mitigation measures subjected to approval of the School.

- 12.14.14. The Contractor shall ensure that access controls are implemented in a fail-secure mode, such that access to the system is not allowed when any part of the System failed.
- 12.14.15. The Contractor shall ensure that credentials (i.e. account ID and password) are provisioned to personnel in such a manner that their confidentiality is maintained.
- 12.14.16. The Contractor shall implement physical security control measures and procedures to prevent any unauthorised access to the System.
- 12.14.17. The Contractor shall not allow remote access to the Systems and network unless the access is properly justified and approved by the School. The Contractor shall implement all the following security measures if remote administrative access is required:
- (a) All remote administration to servers shall be performed from within a management LAN meant only for administration (separate from user traffic);
 - (b) Remote administrative access shall only be performed by authorised personnel from specific systems and access filtering based on IP address shall be implemented. MAC-based access filtering can be implemented as an additional layer of protection over IP-based access filtering;
 - (c) Personnel that are authorised to have remote administrative access shall use multi-factor authentication (MFA) to authenticate to the servers and applications;
 - (d) Logging of date time, IP addresses of the source and destination systems, user information as well as the type of action performed on devices or management consoles implemented by the Contractor for administrative access.; and
 - (e) Remote administrative sessions shall be terminated upon the completion of administration activities.
- 12.14.18. The Contractor shall implement one or more of the approved authentication mechanisms as listed below:
- (a) Authentication using Kerberos, RADIUS, TACACS+, SAML, LDAP, or LDAPS for Windows-based systems or systems supporting Windows application;
 - (b) Certificate-based mutual authentication using at least TLS version 1.2;
 - (c) Authentication using One-Time-Password (OTP) generated by hardware tokens;

- (d) Authentication using digital certificates securely stored in password-protected physical smartcards or hardware tokens;
 - (e) Challenge-Handshake-based authentication using EAP-TLS (RFC-5216) or EAP-IKEv2 (RFC-5106); and
 - (f) Form-based authentication using at least TLS version 1.2.
- 12.14.19. If the Contractor proposes to use authentication mechanisms not listed in Clause 15.22, the Contractor shall provide full technical details and security risk assessments for approval by the School before they are implemented.
- 12.14.20. The Contractor shall ensure the System support strong password administration, secure creation, distribution, termination, storage and destruction of passwords. User's credentials (i.e. User ID and Password) shall be distributed to users in such a manner that their confidentiality is maintained.
- 12.14.21. The Contractor shall ensure the System is implemented with the following features when using passwords:

Creations of Password

- (a) Passwords to be made up of at least **TWELVE (12)** characters;
- (b) Passwords to be made up of **TWO (2)** of the following categories:
 - (i) Upper case alphabet (A through Z);
 - (ii) Lower case alphabet (a through z);
 - (iii) Digits (0 through 9);
 - (iv) Special Characters (!, \$, #, %, etc.);
- (c) Passwords cannot be the same as account ID or user ID;
- (d) Prohibit accepting passwords that are commonly used, guessable or compromised;

Change of passwords

- (a) Passwords to be changed upon the first login;
- (b) Passwords change once every **TWELVE (12)** months;
- (c) Prohibit password reuse for a minimum of **THREE (3)** generations;

Secure usage of passwords

- (a) Protect stored passwords from offline attacks;
- (b) Transmit passwords over an encrypted channel (e.g. Transport Layer Security (TLS), Secure Shell (SSH));

- (c) Passwords must not be displayed in clear;
 - (d) Passwords to be resistant to offline attack when stored by implementing the following:
 - (i) Only password hashes and salts can be stored;
 - (ii) Salt shall be at least 64-bit length;
 - (iii) Salt shall be unique for every password [SP 800-63];
 - (iv) Salt shall be generated using a cryptographically secure random number generator [SP 800-90Ar1, ISO/IEC 19790:2012]
 - (v) Password hashes shall be derived from a suitable one-way Key Derivation function (e.g. PBKDF2). The cost factor should be at least 10,000 iterations.
 - (e) Limit consecutive failed authentication attempts that can be made on a single account to TEN (10) times or less; and
 - (f) Protect internet-facing systems against brute force log-on attempts (i.e. CAPTCHA and delays between failed log-on attempts)
- 12.14.22. The Contractor should ensure the System transmit only cryptographically protected passwords (e.g. encryption of passwords at application layer before transmitting over a secure channel);
- 12.14.23. The Contractor shall ensure the System only return relevant authentication responses for users' reporting purpose only.
- 12.14.24. The Contractor shall ensure use of multi-factor authentication provided by the School for administrators (e.g. system administrator, network administrator, database administrator), operators and other privileged users.
- 12.15. Data Confidentiality and Integrity**
- 12.15.1. The Contractor shall implement control measures that are needed to protect the confidentiality and integrity of security-classified data and other sensitive information (e.g. credentials), subjected to the approval of the School.
- 12.15.2. When requested by the School, the Contractor shall provide detailed description of the control measures.
- 12.15.3. The Contractor shall implement file & folder encryption in the System to prevent administrators or privileged personnel (e.g. system, database and application administrators, etc.) from having access to classified and sensitive data that they are not authorised to access.

- 12.15.4. The Contractor shall implement full disk encryption at key areas (e.g. database servers) of the System where classified or sensitive data is stored, to prevent leakage of classified or sensitive data in the event of device loss at hosting environment.
- 12.15.5. The Contractor shall ensure that all classified data or sensitive data in-transit and at-rest (including backup and archived data) within the System are encrypted with approved cryptographic algorithms.
- 12.15.6. The Contractor shall implement all necessary measures and processes to prevent unauthorised disclosure, modification or deletion of the School's security-classified information.
- 12.16. Personal Data**
- 12.16.1. The Contractor shall take all reasonable measures to ensure that data held in connection with this Contract is protected against loss and against unauthorised access, use, modification, disclosure or other misuse, and that only authorised personnel have access to the data.
- 12.16.2. The Contractor shall use data held in connection with this Contract only for the purposes of fulfilling its obligations under this Contract.
- 12.16.3. The Contractor shall not transfer data held in connection with this Contract outside Singapore or allow parties outside Singapore to have access to it, without the prior approval of the School.
- 12.16.4. The Contractor shall ensure that preliminary drafts, worksheets, storage media and other items containing classified information shall be either destroyed immediately after they have served their purpose or protected as required.
- 12.16.5. The Contractor shall ensure that any employee of the Contractor or any Sub-contractor, requiring access to any data held in connection with this Contract makes an undertaking in writing not to access, use, disclose or retain data except in performing their duties of employment. Failure to comply with this undertaking may be a criminal offence and may lead to disciplinary action against the employee.
- 12.16.6. The Contractor shall immediately notify the School when the Contractor becomes aware of a breach of security in respect to any information held in conjunction with this Contract.
- 12.16.7. The Contractor shall co-operate with the School on any reasonable requests, directions or guidelines of the School arising in connection with the handling of data.
- 12.16.8. The Contractor's personnel shall not access or view the contents of files on the System and equipment (e.g. hard disk or storage media) in the course of their work without prior approval from the School.

- 12.16.9. The Contractor shall work with the School to ensure that data no longer required shall be destroyed in accordance with the School's data disposal guidelines.
- 12.16.10. The Contractor shall work with the School to:
- (a) Prepare the list of personal data collected, used and retained by the System;
 - (b) Analyse the usage, updates and retention of the personal data;
 - (c) Identify the gaps in data protection;
 - (d) Prepare report to document the findings; and
 - (e) Translate the findings into risk statements to be monitored in a risk register.
- 12.16.11. The Contractor shall ensure that database that are not required shall not be made available for public access.
- 12.16.12. The Contractor shall ensure that any employee of the Contractor or any Sub-contractor shall not connect external storage to the servers or System without prior approval from the School.
- 12.16.13. The Contractor shall implement control measures that are needed to protect the confidentiality and integrity of user credentials, which include users' passwords, and other security-classified information.
- 12.16.14. When requested by the School, the Contractor shall provide detailed description of the control measures.
- 12.16.15. The Contractor shall not store or process any classified materials out of Singapore, especially if the nature of the setup is such that the School may not have knowledge of the precise physical location where the materials or information are stored.
- 12.16.16. The Contractor shall put in place necessary processes for managing user access credentials for using online services (for example, user account IDs and passwords), and to make sure that there are proper procedures for hand over and transferring user access credentials due to staff movements (for example, when an officer leaves the company or agency).
- 12.16.17. Classified materials and systems shall be segregated from publicly accessible systems, as well as other third-party, non-School systems.
- 12.16.18. Classified information shall be protected from unauthorised disclosure and tampering during transmission.

12.16.19. All classified data shall be encrypted when transmission is done over public networks (such as internet), or any network links not under the direct control of the School. Cryptographic controls in Clause 17 shall be complied with for data encryption.

12.16.20. The Contractor shall implement the controls listed in the following table:

SAFEGUARDS	Measures
ENCRYPTION-at-rest	Commercially available encryption with no known vulnerabilities
ENCRYPTION-in-transit	
PRIVACY	Not applicable
AUTHORISATION / ACCESS CONTROLS	<ul style="list-style-type: none">• Principle of least privilege (PoLP)• Authorised personnel
LOGGING & MONITORING	<ul style="list-style-type: none">• User access shall be logged• Logs are to be made available to the School upon request

Controls to be Implemented

12.17. Cryptography

12.17.1. The Contractor shall ensure that all proposed cryptographic-based implementations in the System supports minimally the following algorithms or its equivalent. If the Contractor proposes to use cryptography standards not listed below, the Contractor shall provide full technical details and security risk assessments for approval by the School before they are implemented.

12.17.2. The Contractor shall ensure the System uses approved cryptographic algorithms as follows:

Cryptographic Type	Type of Algorithm	Cryptographic Strength
Cryptographic Hashing Algorithm	Secure Hash Algorithm 3 (SHA-3)	At least SHA3-256
	Secure Hash Algorithm 2 (SHA-2)	At least SHA2-256
Symmetric-Key Algorithm	Advanced Encryption Standard (AES)	At least AES-128 Galois Counter Mode (GCM) shall be used where possible, Electronic Code Book (ECB) shall not be used, and Cipher Block Chaining (CBC) shall not be used when using TLS.
Public-Key Cryptography	Elliptic Curve Cryptography (ECC)	1. At least P-256 2. Curve Curve25519 or 3. Curve448
	Rivest-Shamir-Adleman (RSA) Public Key Encryption	Key size of at least 2048-bits
Digital Signature Algorithm	Digital Signature Algorithm (DSA)	L at least 2048, N at least 224 Where L is the bit length of the prime modulus N is the bit length of the prime divisor
	Elliptic Curve	1. For IKE v2, at least P-256

	Cryptography Digital Signature Algorithm (ECDSA)	2. For TLS, at least B-233, K-233 or P-256
	RSA Probabilistic Signature Scheme (RSA-PSS)	Use key size of at least 2048-bits
Key Exchange	Elliptic Curve Diffie-Hellman (ECDH)	1. For IKE v2, at least P-256 2. For TLS, at least B-233, K-233 or P-256
	Finite Field Diffie-Hellman (FFDH)	1. For IKE v2, at least MODP-3072 (ID=15) 2. For TLS, at least ffdhe3072 (ID=257)
Key Wrapping	Advanced Encryption Standard (AES)	At least AES-128
Random Bit Generation (RBG)	Hash-based Deterministic Random Bit Generator Hash_DRBG	Any hash functions specified in FIPS-180 or FIPS-202.
	HMAC-based Deterministic Random Bit Generator HMAC_DRBG	Any hash functions specified in FIPS-180 or FIPS-202.
	Counter Deterministic Random Bit Generator CTR_DRBG	At least AES-128.
Message Authentication Code (MAC)	Keyed-hash MAC (HMAC)	Implemented with approved cryptographic hash algorithms.
	Cipher-hash MAC (CMAC)	Implemented with approved AES algorithm.
	Galois MAC	Implemented with approved AES algorithm.

- 12.17.3. The Contractor shall ensure the implementation of digital certificate and certificate revocation lists shall comply with X.509 v3 standard.
- 12.17.4. The Contractor shall ensure all digital certificates implemented within the System are from a trusted Certificate School designated by the School. The Contractor shall ensure no self-signed certificates is used in the System unless approved by the School.
- 12.17.5. The Contractor shall ensure cryptographic materials generation events are logged in the audit trail and access to cryptographic materials generation function shall be authenticated.
- 12.17.6. The Contractor shall ensure that cryptographic mechanisms implemented in the System can handle the peak loads without degrading the performance of the System.
- 12.17.7. The Contractor shall ensure that cryptographic materials (e.g. keys, seed, hash, etc.) used within the System are always protected, such that there is no unauthorised access or decrypting / deriving the information protected by these cryptographic materials.
- 12.17.8. The Contractor shall ensure that cryptographic keys and passwords are not hard-coded in the System, and are not made known to unauthorised person.
- 12.17.9. The Contractor shall develop, implement and maintain a key management process specific to the System as follows:
- (a) Cover key generation, registration, storage, distribution, installation, usage, rotation, backup, recovery, revocation, suspension, and destruction;
 - (b) Seek approval from the School before implementation;
 - (c) After development and implement, review and update the key management process annually or otherwise determined by the School; and
 - (d) Seek approval from the School for subsequent updates.
- 12.17.10. The Tenderer shall propose a key management system for the System, in-line with the Clause 12.17.9 key management process to ensure that all cryptographic keys and materials are securely stored and managed. In the event the Tenderer is unable to propose a key management system due to technical limitations, the Tenderer shall propose alternate mechanism including process control to manage the keys, subjected to approval of the School. The Contractor shall implement and maintain the approved key management system or alternate mechanism.
- 12.17.11. The Contractor shall ensure all direct access to cryptographic keys and materials in the System at any time are logged.

- 12.17.12. The Contractor shall ensure that the System allows proper backup and recovery of cryptographic keys. The Contractor shall work with the School-appointed Contractors to ensure periodic testing of the backup and the recovery process to verify that cryptographic keys can be recovered within the stipulated timeframe.
- 12.17.13. The Contractor shall ensure cryptographic keys used to protect data are encrypted and stored in secure protected storages or be minimally secured in cloud native key management tools which are certified FIPS 140-2 Level 2 or higher.
- 12.17.14. The Contractor shall define the certificate generation template and obtain approval from the School.

12.18. Information Backup Security

- 12.18.1. The Contractor shall ensure access of all backup administrators to the backup System shall require strong multi-Factor Authentication (MFA).
- 12.18.2. The Contractor shall ensure the proposed backup solution maintain the access rights of the source data onto the backup data.
- 12.18.3. The Contractor shall ensure the proposed backup solution maintain the same integrity state of the source data onto the backup data.
- 12.18.4. The Contractor shall ensure the proposed backup solution ensure the confidentiality and integrity of all backup data.
- 12.18.5. The Contractor shall ensure a copy of the backup data is kept offline so that the System can be recovered in the event of a successful ransomware attack.

12.19. Change Management and Patch Management

- 12.19.1. The Contractor shall ensure that any changes to the original design, implementation and setup of the System are approved by the School before making the change.
- 12.19.2. The Contractor shall propose and implement a change control process, subjected to the School's approval, to ensure that all intended changes to the original configurations and/or changes to the production environment are properly reviewed, tested in UAT environments, authorised before implementations, and verified properly implemented.
- 12.19.3. The Contractor shall provide detailed description of the change control process, which shall at least include the people involved in the reviewing, authorising and implementing the change, the System products or solutions used if any.

- 12.19.4. The Contractor shall implement and operate the necessary infrastructure and processes to control the deployment and maintenance of software releases into the System. This is to help keep the System up-to-date, and to overcome known security vulnerabilities.
- 12.19.5. The Contractor shall develop and maintain a security patch management plan that is specific to the System, which includes the monitoring of availability of security patches and the actions needed to address the System vulnerabilities, the timeline and the function responsible for reviewing or testing, authorising and implementing the security patches.
- 12.19.6. The Contractor shall implement and adhere to the approved Patch Management process which shall consist at least the following phases:
- (a) Assessment of the environment,
 - (i) System baselining;
 - (ii) Asset inventory;
 - (iii) Patch management architecture;
 - (iv) Infrastructure and configuration review;
 - (b) Identification of new software update,
 - (i) Identify new patches;
 - (ii) Determine patch relevance;
 - (iii) Verify patch authenticity and integrity;
 - (c) Evaluation and planning of software update, and
 - (i) Impact analysis;
 - (ii) Patch acceptance testing;
 - (iii) Patch deployment plan and approval;
 - (d) Deployment of software update.
 - (i) Patch deployment;
 - (ii) Progress report;
 - (iii) Exception handling; and
 - (iv) Deployment review.
- 12.19.7. The Contractor shall proactively monitor information about new software updates on a monthly basis.
- 12.19.8. The Contractor shall determine whether the software update should be considered a normal change or an emergency one.

- 12.19.9. The Contractor shall submit a request for change to the School to seek approval to deploy the software update. The submission of the request to the School shall be completed within ONE (1) calendar day from the time the official patch is made available by the vendor to the time request is received by the School.
- 12.19.10. The Contractor shall ensure security and relevant patches, when released officially by the vendors or when notified by the School, are applied to the System in a timely and controlled manner, within the implementation timeframe specified in table below:

Type of System	Type of Patch	Deployment upon availability of Patch
All	Emergency	TWENTY-FOUR (24) hours
1. Internet-accessible Application Systems	High	THIRTY (30) calendar days
	Medium / Low	SIXTY (60) calendar days
2. Intranet Application Systems	High	SIXTY (60) calendar days
	Medium / Low	NINTY (90) calendar days

- 12.19.11. The Contractor shall submit the test results to the School to seek approval for deployment to production environment. The submission shall include a rollback plan. The submission shall also include any forward schedule of change and user communications messages.

12.20. Vulnerability Management

- 12.20.1. The Contractor shall assess all security vulnerabilities, whether reported to it or uncovered by its own means, and provide an assessment and report to the School.
- 12.20.2. The Contractor shall ensure the assessment include a determination of the threat posed by the vulnerability, its impact and its severity.
- 12.20.3. The Tenderer shall provide details of and implement the security measures to prevent malicious codes from harming the System and networks.
- 12.20.4. The Contractor shall ensure that vulnerability assessment using industry recognised tools is performed on the System on a quarterly basis.
- 12.20.5. The Contractor shall obtain security patches from authorised sources and verify their integrity before working with the School to test and apply the patches.
- 12.20.6. If any vulnerability is found to be due to parts and components supplied by the Contractor, the Contractor shall provide remedial actions to rectify the problem at no additional cost to the School.

12.21. Systems using Commercial Cloud

- 12.21.1. The Contractor shall implement logging of all security-related events such as:
- (a) Privileged account activities (i.e. administrations, configuration changes, application/system policy changes, or API access permission changes);
 - (b) Logon, logoff and usage activities (i.e. abnormal logon attempts, logon success and failures, escalation of privileges, certificate activities);
 - (c) Database activities (i.e. configuration changes, account and access rights activities, connection attempts, database errors); and
 - (d) Network activities (i.e. traffic to/from malicious network addresses or domain names, suspicious outbound connections, rejected and dropped network traffic).
- 12.21.2. The Contract shall implement the following security measures:
- (a) Cloud native network firewalls (i.e. AWS Security Groups, Azure Network Security Groups, Google Armor)
 - (b) Cloud security detection tools (i.e. AWS GuardDuty, Azure Sentinel, Google Stackdriver)
 - (c) Cloud native logging whenever possible (i.e. AWS CloudWatch, Azure Audit logs, Google VPC Flow logs)
 - (d) Notification when suspicious activities are detected; and
 - (e) Stream logs to central logging servers.
- 12.21.3. The Contractor shall be certified with either CSA-STAR or all three of ISO-27001, ISO-27017 and ISO-27018.
- 12.21.4. The Contractor shall ensure they are audited by independent third parties according to SOC standards at least once annually.
- 12.21.5. The Contractor shall implement the following key management measures:
- (a) Ensure cryptographic keys are rotated regularly (e.g. every SIX (6) months, annually);
 - (b) Ensure that all the accounts that are granted with the permission to manage and administrate the keys are regularly reviewed according to the agency's requirement, and remove all excessive permissions timely; and
 - (c) Ensure proper process when managing cryptographic key policies (e.g. key lifecycle, key allocations, key rotation).
- 12.21.6. The Contractor shall implement the following data security measures:

- (a) Ensure that data at rest is encrypted (e.g. block, file, directory and snapshot level);
- (b) Ensure data in-transit is encrypted over untrusted networks;
 - (i) Use of encrypted channel for communication over the Internet or any other untrusted networks (e.g. HTTPS, TLS, IPSec, SFTP).
- (c) Identify all possible data flows and critical path;
 - (i) Details of all communication channels of the residing data (e.g. TCP traffic, API calls, Intranet and Internet Compartments).
- (d) Ensure data are segregated according to agency's requirements and environment;
 - (i) Ensure all data are separated clearly according to agency's project environment. (E.g. Pro, Non-Pro, UAT, Development, Operations).
- (e) Ensure data life span is kept in accordance with agency's requirements; and
- (f) Ensure data that has reached its end of its lifecycle is securely deleted;

12.21.7. Delete both the encrypted data and their corresponding encryption keys in their storages, when data is no longer required.

12.22. Logging and Audit Trails

- 12.22.1. The Contractor shall implement facility to store all logs (i.e. application, database, network, Operating System, security, etc.) of the System, including logs from servers, applications, network appliances and security solutions, etc.
- 12.22.2. The Contractor shall ensure that sensitive information (e.g. password) is not stored in the logs.
- 12.22.3. The Contractor shall ensure that logs are accessible to authorised personnel only.
- 12.22.4. The Contractor shall ensure the System is implemented with logging mechanism to log all activities in the System including actions performed by privileged user accounts (for e.g. system administrators, auditors, and database administrators). The activities to be logged minimally include the following: —
- (a) User administration activities (e.g. add / delete / amend user accounts and profiles);
 - (b) Privileged user activities in application (e.g. add / delete / amend application configurations);
 - (c) System administration activities (e.g. add / delete / amend system configuration);

- (d) Database activities (e.g. configuration change, account and access rights activities, connection attempts, database errors);
- (e) Network activities (e.g. configuration traffic to and from malicious network addresses or domain names, suspicious outbound connections, rejected and dropped network traffic);
- (f) System backup and recovery activities;
- (g) User log in and out activities;
- (h) Successful and unsuccessful attempts to logins and logouts of the System;
- (i) Use of privileged functions and utilities;
- (j) Access violations from local and remote requests;
- (k) Service start up and shutdown;
- (l) Service backup and recovery; and
- (m) Configuration changes.

12.22.5. The Contractor shall ensure the System is capable of logging transaction performed by users (e.g. adding, editing, and deletion of records, cases, documents). The School reserves the rights to decide on the types of user activities to be logged in the audit trails.

12.22.6. The Contractor shall ensure information in audit logs contain minimally the following: —

- (a) Date of transaction;
- (b) Time of transaction;
- (c) Source of occurrence;
- (d) Account and name who made the transaction;
- (e) Information before and after the transaction;
- (f) Online screen reference/id if changes were made online; and
- (g) Batch job reference/id if changes were made in batch.

12.22.7. The Contractor shall identify and include additional information for the audit log if necessary.

12.22.8. The Contractor shall ensure that the individual actions of all personnel working on the System are accounted for and auditable.

- 12.22.9. The Contractor shall enforce segregation of roles to ensure that roles that can review logs have no rights to any other part of the System except to the Log Repository solution.
- 12.22.10. The Contractor shall implement tamper protection measures to safeguard the integrity of logs and audit trails, e.g. intentional abuse or unintentional misuse through modification or deletion, no access to logs by operations personnel to prevent risk of tampering or deletion. The protection measures are subjected to the approval of the School.
- 12.22.11. The Contractor shall synchronise the System's clock / time to a common, accurate and secured time source.
- 12.22.12. The Contractor shall ensure the System keeps these logs for at least ONE (1) year. For network packets and flows, the logs shall be kept for at least ONE (1) calendar month and THREE (3) calendar months respectively.
- 12.22.13. The Contractor shall ensure the System prompt authorised users to archive the audit trails when the records reach or exceed the retention period.
- 12.22.14. The Contractor shall provide and maintain a backup or archival plan specifying details on the frequency and method to backup or archive the logs. The backup or archival plan shall be subjected to approval of the School
- 12.22.15. The Contractor shall ensure the System present the logs in a format that is easy to read by authorised users, such as ASCII or UTF-8 encoded text files.
- 12.22.16. The Contractor shall implement process for all necessary logs to be reviewed monthly or when necessary, such as after configuration changes to scan for security violations, issues or concerns and highlight them to the School. The Contractor shall use automated tools for log review, where possible.
- 12.22.17. Upon notification by the School or the School appointed parties, the Contractor shall make available the logs of the requested systems in accordance to the following schedule:

Age of logs	Turnaround Time
Up to THREE (3) months old	Within ONE (1) calendar day
More than THREE (3) months old	Within FIVE (5) calendar days

Table 3: Turnaround Time for Logs

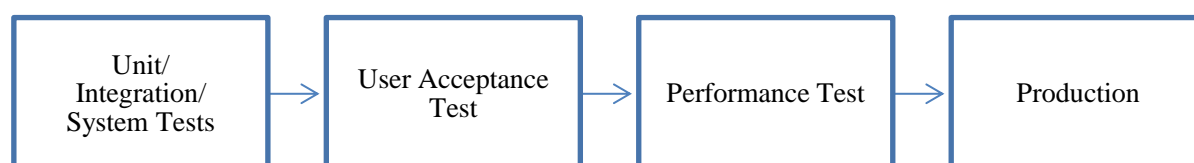
13. TESTING, SYSTEM DELIVERY AND ACCEPTANCE REQUIREMENTS

13.1. General Requirements

13.1.1. The Contractor shall conduct acceptance tests on the entire System including the Hardware and Software to verify and demonstrate that the System meets the Requirement Specifications (“Acceptance Tests”). In this Tender Offer, the Tenderer shall propose various operational implementation phases for the System (“**Implementation Phases**”), which is subject to the review and confirmation of the School.

13.1.2. The Contractor shall follow the approval / vetting process shown in the diagram below for the migration of applications from one environment to the next. The details of the process will be given to the Contractor:

Figure 3: Approval / Vetting Process for Migration of Application



13.1.3. The relevant Acceptance Tests shall be performed:

- (a) on the System prior to the implementation of each Implementation Phase/Commissioning Date; and
- (b) on enhancements made to the System pursuant to Service Requests raised by the School during the Life-Span of the System.

13.1.4. The Acceptance Tests shall also apply to substitute, replacement and conversion of any component parts that are acquired by the School in relation to this Contract.

13.1.5. The Contractor shall include the list of quality metrics indicated in the table below as part of the Master Test Plan.

QA Aspect of Quality Metrics
Unit Test Coverage Percentage code coverage percentage – To achieve as high coverage as possible e.g. recommended 70-80%. Coverage criteria – e.g. statement, condition or branch coverage.

QA Aspect of Quality Metrics
For Manual Test Case <ul style="list-style-type: none"> Planned versus actual test case creation Planned versus actual test case execution Test Case Execution Status (e.g. by total number of test cases executed, passed, failed and blocked).
For Automated Test Case <ul style="list-style-type: none"> Planned versus actual test script creation Planned versus actual test script execution Percentage of Automated Test = Number of automated test / Total number of test cases (manual & automated) * 100% Total Test Duration - Measure the total test duration to run the automated tests, to look for a trend over a period of time and watch out for sudden increase Test Script Execution Status (e.g. by total number of test script executed, passed, failed and blocked).
Defect trending (e.g. by severity, priority, aging, status) Regular report should be provided for defect trending.

- 13.1.6. The Tenderer shall prepare and submit with the Tender Offer a Preliminary Master Test Plan for the proposed System. The purpose of this Preliminary Master Test Plan is to ensure that the Tenderer has considered all test requirements specified in the Tender documents and has made adequate provisions for testing. The Preliminary Master Test Plan shall also demonstrate the Tenderer's understanding of the range, depth and other aspects of the tests to be conducted.
- 13.1.7. Following award of the Contract, the Contractor's Preliminary Master Test Plan in its Tender Offer shall be updated in consultation with the School and shall be re-submitted to the School for approval as the Master Test Plan. The Master Test Plan will be updated with greater detail of the planned test dates throughout the course of the project.
- 13.1.8. The Contractor shall provide evidence that the System complies with or exceeds the Requirements Specification using test methods such as code review, unit testing, systems integration testing, performance and load testing. The test evidence shall include details such as test scenarios, cases and results, infrastructure health (e.g. network utilisation, CPU, RAM, I/O etc.), software/middleware health (e.g. application server, rules engine, service bus etc.) and application health (e.g. java heap utilisation, connection pools etc.) so as to provide 360 perspective including environmental information. The Contractor shall analyse the test results and evidence to include environmental health and remediation action if any.

- 13.1.9. The Contractor shall note that the appointment of the Test Consultant is subject to the School's approval.
- 13.1.10. The Contractor shall bear the cost of all the Test Consultant's services and related consultancy services.
- 13.1.11. The Test Consultant shall not be part of the development team or be involved in any development work during the whole duration of the project.
- 13.1.12. The Contractor shall use testing tools to uncover any defects in the early stages of development to ensure that defects detected are rectified promptly and permanently, including the identification and eradication of any potential upstream and downstream impact. The Tenderer shall state the testing tools to be used in the Tender Proposal.
- 13.1.13. The Contractor shall provide development checkpoints to demonstrate to the School Representative that the modules developed are according to the functional requirements. The Contractor shall propose the modules to be presented at each development checkpoint, subject to the School's approval.
- 13.1.14. The Contractor shall allow the School to inspect the Contractor's development work / partially completed system / completed modules in the Contractor's SIT environment during the development checkpoints.

13.2. Test Levels and Test Types

- 13.2.1. The Acceptances Tests shall include the following test levels:

Test Levels	Description
Unit Testing	Level of the software testing process where individual units/components of a software/system are tested. The purpose is to validate that each unit of the software performs as designed.
System Integration Testing (SIT)	Level of the software testing process where a complete, integrated system/software is tested. The purpose of this test is to evaluate the System's compliance with the specified requirements.
User Acceptance Testing (UAT)	Level of the software testing process where a system is tested for acceptance. The purpose of this test is to evaluate the System's compliance against the Signed-off Functional and Design specifications and assess whether it is acceptable for delivery.

- 13.2.2. Each of the test levels can include one or more of the following test types:

- (a) Unit Test
- (b) Source Code Review

- (c) Compliance Test
- (d) Usability Test
- (e) Functional Test
- (f) Data Conversion & Migration Test
- (g) Integration Test
- (h) Performance Test
- (i) Security Test
- (j) Operational Readiness Test

13.2.3. The following table shows the test types applicable for each test level:

Table 4: Test Types for Applicable for each Test Level

Test Types	Test Levels		
	Unit Testing	System Integration Testing	User Acceptance Testing
Unit Test	x		
Source Code Review	x		
Compliance Test		x	x
Usability Test			x
Functional Test		x	x
Data Conversion & Migration Test		x	x
Integration Test		x	
Performance Test		x	x
Operational Readiness Test			x

13.2.4. The Preliminary Master Test Plan shall include the details of all tests necessary to assure that the System meets the Requirement Specifications in all aspects, especially the security, performance and functionalities of the System. It shall include, at the minimum, plans for the test levels and test types described above.

13.2.5. The Contractor shall update the Master Test Plan, or provide additional test plan documentation, for approval by the School no later than TWO (2) months prior to the actual conduct of the respective tests (unless otherwise expressly specified herein).

- 13.2.6. The Master Test Plan shall include the time schedule and sequence of events necessary for the acceptance of the System, including a delivery schedule for the documentation and the respective dates for development, testing, installation, delivery and acceptance of the System. The schedule shall not conflict or contradict with the Implementation Plan.
- 13.2.7. The Master Test Plan, and any updates therein, is subject to the School's review and approval. The School reserves the right to modify the Master Test Plan, e.g. the scope of testing, and to specify different or additional procedures or tests to be conducted within the scope of the Contract.
- 13.2.8. The Contractor shall provide all hardware, software, hosting, infrastructure, equipment and services required for the System Integration Testing ("SIT") and development environments. The SIT and development environment shall be provided by the Contractor at no additional cost to the School.
- 13.2.9. The Contractor shall provide all the SaaS, software, licenses and services required for the execution of all Acceptance Tests.
- 13.2.10. The Contractor shall make the necessary arrangements to enable the representatives of the School to observe the Acceptance Tests in order to verify that the said tests are properly carried out.
- 13.2.11. The Contractor shall conduct the Acceptance Tests in compliance with the Security Clauses in **Clause 0**.
- 13.2.12. Acceptance Tests shall be carried out at the School selected UAT environment only after testing has been completed successfully by the Contractor at the development and SIT environments. The Contractor shall submit the test results to the School for verification prior to installing the new, or enhanced, or debugged applications or patches into the staging environment in School selected UAT environment.
- 13.2.13. The Contractor shall conduct, at the development environment, all the necessary test types leading up to the System Integration Tests (SIT) and User Acceptance Tests (UAT).
- 13.2.14. The signing of the User Acceptance completion signifies the acceptance by the School of the System and is, subject to such reservations as may be endorsed thereon by the School, final and binding in respect of all matters covered by the Acceptance Tests.
- 13.2.15. When tests are to be conducted with high frequency and where feasible, the Contractor shall automate the execution of tests to reduce execution time and minimize variance between test runs.
- 13.3. Test Level: Unit Testing**
- 13.3.1. Development Environment

- 13.3.1.1. The Contractor shall propose the setup of the required development environment at the Contractor's premises in Singapore for the purpose of testing the development of and enhancements to the System, and to conduct SIT, at no charge to the School.
- 13.3.1.2. The Contractor shall perform the Acceptance Tests in the development environment and submit the test results to the School for review and acceptance prior to installing the new, enhanced or debugged applications or patches into the staging environment in School selected UAT environment site.
- 13.3.1.3. The Contractor shall carry out the Acceptance Tests at the School selected UAT environment site once the staging environment is setup there.

13.4. Test Level: System Integration Testing (SIT)

- 13.4.1. Before the SIT is performed by the Contractor, the Contractor shall produce the updated Master Test Plan or SIT Plan to the School for review and approval at least TWO (2) months in advance. The Contractor shall provide test cases/ scenario documents in the Master Test Plan or SIT Plan and map them to the individual functions of the signed-off functional/ requirements specification to ensure completeness and comprehensiveness of the test cases/ scenarios.
- 13.4.2. The Contractor shall submit documental proof to the School for the successful completion as well as test results for the SIT, e.g. tested the functionalities, performance, stability and resilience of the various components of the System prior to UAT.
- 13.4.3. The Contractor shall conduct the tests on the System in the testing environment to ensure that the software and hardware have been installed and setup properly.
- 13.4.4. The scope of the SIT shall cover functional, interfacing and integration tests on all units/ modules developed in the System as well as system Software, including all customisations done, to ensure all requirements/ functionalities, performance, stability and resilience of all components in the System have been thoroughly tested and met.
- 13.4.5. At the end of the SIT, the Contractor shall prepare the SIT report detailing the test cases, test results (both expected and actual test results), problems identified and rectification actions taken.
- 13.4.6. The Contractor shall submit the SIT report at least TWO (2) weeks before the commencement of the UAT. The School reserves the right to hold back the UAT until the evidence of the successful completion of the SIT is produced.
- 13.4.7. During SIT, the Contractor shall provide weekly updates on the SIT progress in accordance with the School's directions.

13.5. Test Level: User Acceptance Testing (UAT)**13.5.1. Pre-UAT Test**

13.5.1.1. The Contractor shall ensure that the UAT environment is available for the School to conduct a Pre-UAT Test prior to the start of UAT.

13.5.1.2. The Pre-UAT Test will be conducted by the School based on a random sampling of functional test cases and scenarios.

13.5.1.3. If the School is not satisfied with the result of the Pre-UAT Test then the School may, by written notice to the Contractor elect at its sole option:

- (a) to have the Pre-UAT Test extended (without prejudice to its other rights and remedies) on the same terms and conditions within a reasonable time. Unless otherwise agreed in writing between the Parties, all such extensions shall not be construed as any grant of extension of time by the School and the Contractor remains liable for any delay in complying with its obligations under the Contract; or
- (b) to have the System Integration Tests repeated (without prejudice to its other rights and remedies) on the same terms and conditions within a reasonable time. Unless otherwise agreed in writing between the Parties, all such repeat System Integration Tests shall not be construed as any grant of extension of time by the School and the Contractor remains liable for any delay in complying with its obligations under the Contract; or
- (c) to direct the Contractor to make specific rectifications to the UAT environment (without prejudice to its other rights and remedies) within a reasonable time. The Contractor shall bear all costs for such rectifications. Unless otherwise agreed in writing between the Parties, all such rectifications shall not be construed as any grant of extension of time by the School and the Contractor remains liable for any delay in complying with its obligations under the Contract.

13.5.2. Test Plan and Test Cases

13.5.2.1. The Contractor shall design test cases (including unit functional testing and scenarios testing) in the Master Test Plan or UAT Plan to demonstrate the capability of the proposed System to survive and handle erroneous inputs in a proper manner. The inputs shall include invalid data or a combination of these to test the error handling mechanisms built into the System. The Contractor shall be expected to run through the test cases with the users who will be participating in the UAT (“UAT Users”) before finalising the test cases. The Contractor shall draft the test cases based on the sign-off functional/ requirements specification and allow the School to review/ add in more business test scenarios to test the functionality/ capability of the System.

13.5.3. Preparing for UAT

- 13.5.3.1. The Contractor shall provide training for UAT users in order to guide them on how to conduct the tests.
- 13.5.4. UAT Environment
- 13.5.4.1. The Contractor shall be responsible for the setup of the entire UAT environment at no charge to the School, including the necessary infrastructure, hardware, hardware peripherals, network, system software, interfaces etc. In addition, the Contractor shall also be responsible for the setup of the UAT users' testing environment including the infrastructure, network, clients (PCs, notebooks, mobile devices etc), clients software, etc. as well as logistics, e.g. location(s), UAT testing schedules/ hours.
- 13.5.4.2. The Contractor shall also be responsible for the preparation and refresh of the required test datasets for the independent testing and test cases in the UAT. The Master Test Plan or UAT Plan and schedule shall be communicated at least ONE (1) month before start of UAT, to allow UAT users ample time to plan their operations work such as to avoid clashes with the UAT schedule.
- 13.5.4.3. The Contractor shall ensure that the UAT environment is set up in time for the UAT to commence as scheduled.
- 13.5.4.4. The Contractor shall prepare a plan for the setup and configuration of the UAT environment, including the hardware and system software, which are required to implement the proposed System. The UAT setup and configuration plan shall be submitted for the School's approval at least TWO (2) months before the UAT.
- 13.5.4.5. The Contractor shall deploy the proposed System in the UAT environment according to the installation plan. This shall help to serve as a testing platform for the installation plan to ensure that the installation plan is correct, accurate and complete for later use in the deployment to the production environment.
- 13.5.4.6. The Contractor shall do the necessary set-up (e.g. creation of test data) to demonstrate that the proposed System can meet the performance requirements under peak testing load when operated in the UAT environment.
- 13.5.4.7. The UAT environment shall be similar to the configuration of the Production environment so that results of tests carried out in the UAT environment are consistent with that in the production environment. The expected load for UAT environment shall be one quarter of the production load.
- 13.5.5. Conducting UAT
- 13.5.5.1. The Contractor shall provide a full-time, qualified, and competent team with relevant experience on-site to take charge of the UAT. The team shall work closely with UAT users to follow through all the testing required and to document the UAT process. The UAT team shall provide advice and assistance to UAT users in conducting the test cases during the UAT. The UAT team shall whenever possible, resolve the bugs reported so that the reporting UAT users

could quickly retest the failed test case. In the event of more complex bugs, the UAT team shall escalate to the development team for solutions. Once the solution(s) are ready, the UAT team shall co-ordinate with the respective UAT users for retesting.

- 13.5.5.2. The Contractor shall document all UAT defect logs and consolidate the defects into a summary with the required details on cause of problem, proposed resolution actions and timeline for such actions for approval by the School. The Contractor shall facilitate monitoring of defects fixing, re-testing and proper closure according to the approved timeline. The Contractor shall also track the defect ratio (e.g. % of failure against % of total test scope).
- 13.5.5.3. The Contractor shall update the consolidated defect log daily and submit the updated consolidated defect log to the School by noon the following working day. The Contractor shall conduct UAT debrief at the end of each day with the School and School representatives on every consolidated defect log during the UAT period.
- 13.5.5.4. The Contractor shall propose a mechanism to prioritise, assign, track, report and audit defects reported at UAT. The Contractor shall provide weekly update on the UAT progress. Every defect reported during UAT must be rectified before commencing the next round of UAT. This is to ensure that all defects reported are followed up with and resolved with successful testing.
- 13.5.5.5. For major enhancements, the Contractor shall conduct a UAT briefing at least FIVE (5) working days before the test commencement date. The Contractor shall also conduct a UAT debrief session at the end of each UAT day to consolidate the incidents obtained as well as to review the UAT progress.
- 13.5.5.6. The UAT shall not be deemed completed until all the tests and documentations are accepted and signed off by the School.
- 13.5.6. UAT Reports and Acceptance
- 13.5.6.1. At the end of the UAT, the Contractor shall prepare the UAT report detailing the test cases, test results (both expected and actual test results), problems identified and rectification actions taken.
- 13.5.6.2. The UAT report shall be submitted to the School within **FIVE (5)** working days after the end of the UAT for review for the School's approval and sign-off by the School, before the proposed System is rolled out to production environment.
- 13.5.6.3. In the event of non-compliance with requirements specification or the user acceptance criteria, the proposed System may be rejected by the School. The Contractor shall take immediate action to analyse the failure and rectify the problem discovered. The Contractor shall meet the following resolution times which depend on the severity of the defect:

Table 5: Severity Level and Resolution Time

Defect Severity	Description	Resolution Time
1	Defects that are show-stoppers to the UAT and need to be resolved for UAT to continue.	Within ONE (1) working day
2	Defects that are not show-stoppers to the UAT but affect majority (> sixty percent (60%)) of the scenarios.	Within THREE (3) working days
3	Defects that are not show-stoppers to the UAT and affect only some scenarios.	Within FIVE (5) working days
4	Defects that are not critical and do not affect UAT progress nor go-live.	Within TEN (10) working days

Depending on the nature/complexity of the defect, the Contractor may request for a mutually agreed timeframe that differs from the above resolution times.

- 13.5.6.4. If the acceptance criteria is not met at the end of the UAT duration, the Contractor shall provide additional rounds of UAT till the acceptance criteria is met. The duration of each additional round of UAT shall be determined by the School. The cost of the additional rounds of UAT will be borne by the Contractor and the Contractor will also be held accountable for the delay. If the rate of defect resolution is deemed unsatisfactory to the School, the School may call a halt to the UAT and the Contractor shall be held fully accountable for the delay and the subsequent failure to meet the implementation schedule.

13.6. Test Type: Unit Tests

- 13.6.1. The Contractor shall carry out the unit tests at the development environment to ensure that each unit/ module developed for the System has met the Requirement Specifications and is stable.
- 13.6.2. The Contractor shall ensure that the unit tests cover all aspects of the code, including configuration required to support the code. Examples include:
- (a) Aspect of the programming: variables, type and logic;
 - (b) Program objects such as classes or objects, reusable components, common libraries;
 - (c) Non-functional aspect: batch job, scripts; and
 - (d) Product specific customisation or configurations.
- 13.6.3. The Contractor shall provide the unit tests results to the School for review and acceptance not later than **SEVEN (7)** days from the completion of the tests. The Contractor shall ensure that the Unit Tests covers the different possible scenarios such as:

- (a) Test usage by the different users or actors
- (b) Time sensitivity test e.g. cross over year, leap year, business work year versus calendar work year
- (c) Boundary values cases
- (d) Input data validation (e.g. check that field accepts allowable characters only)
- (e) Security (e.g. Verifying permissions and access to objects, testing robustness against cross-site scripting payloads)
- (f) Business requirements in term business rules, and exception handling such as business calendar versus working period

13.6.4. If the test is unsuccessful, or the School considers the test results to be unsatisfactory, the Contractor shall follow-up to make the necessary changes to the relevant unit/module and re-perform the unit tests.

13.6.5. The Contractor should implement automated unit testing as part of the daily build.

13.7. Test Type: Source Code Review

13.7.1. The Contractor shall propose the process policy, appropriate tools and frequency to perform source code review and shall submit the proposal to the agency for review and approval.

13.7.2. The Contractor shall propose the coding guidelines, inclusive of best practices, that shall be adhered to when developing and reviewing the Application Software.

13.7.3. The Contractor's coding guidelines shall include the following aspects as necessary:

- (a) Language specific guidance, e.g. preventing buffer overflows in C++
- (b) Framework and / or product specific guidance, e.g. enable ASP.NET's request validation for all HTTP requests
- (c) Security, e.g. usage of security libraries to prevent XSS
- (d) Quality and maintainability, e.g. coding style and conventions

13.7.4. The Contractor shall take reference from authoritative sources in coming out with its coding guidelines, such as from the product principal, e.g. Oracle's ADF coding guidelines.

- 13.7.5. The Contractor may rely on the use of tools to enforce adherence to aspects of its coding guidelines.
- 13.7.6. The Contractor shall review and refine its coding guidelines as necessary to maintain the effectiveness of its development and review processes.
- 13.7.7. Manual Source Code Review
- 13.7.7.1. The Contractor shall ensure that all source code developed by the Contractor or its sub-contractors are reviewed manually to ensure that the source code fulfils software requirements, quality, performance and security standards.
- 13.7.7.2. The Contractor shall ensure that critical and / or sensitive segments of code are subjected to a higher level of scrutiny. This includes code for key business functions and security controls. This shall be described in the Contractor's proposed process policy.
- 13.7.7.3. Manual source code review may be segmented, conducted incrementally and paced throughout the development lifecycle to facilitate that all code is reviewed effectively. This shall be described in the Contractor's proposed process policy.
- 13.7.7.4. The Contractor shall ensure that source code review and follow up actions are completed prior to code deployment to the production environment.
- 13.7.7.5. The Contractor's proposed process policy for manual source code review shall define at minimum the following:
- (a) When a review shall be conducted and on what piece of code, e.g. on every code change prior to inclusion into the source code repository,
 - (b) Whom a review shall be conducted by, e.g. by a technical lead or by 2 peers,
 - (c) How a review shall be conducted, e.g. code walkthrough with code author,
 - (d) What is examined in a review and methodology for examination, e.g. code style, quality and security,
 - (e) How code reviews are captured and documented, and
 - (f) How follow-up actions are captured, tracked and closed.
- 13.7.7.6. The Contractor shall ensure that the following aspects are examined in its manual source code review:
- (g) Completeness of task, e.g. tests are present, code is documented
 - (h) Correctness, e.g. fulfilment of functional requirements, checks for business logic errors
 - (i) Adherence to coding guidelines

(j) Inspection for security vulnerabilities

13.7.7.7. The Contractor shall take reference from established and current security sources in deriving its methodology for reviewing its code for security, such as from the Open Web Application Security Project (OWASP) Code Review Guide.

13.7.7.8. The Contractor shall provide evidence of the code review at the School's request.

13.7.8. Static Code Analysis

13.7.8.1. The Contractor shall make use of automated source code scanning tools and propose a regular frequency to perform static code analysis of at least once upon each change to ensure that the source code meets minimum quality and does not contain programming errors such as, but not limited to, the following:

(a) Improper Input and Output Validation

(b) Cross-site Scripting

(c) SQL Injection

(d) OS Command Injection

(e) Improper Session Management

(f) Buffer Overflow

(g) Code Injection

(h) Insecure File Path/ Name

(i) Improper Initialisation

(j) Modification of Critical State Data

(k) Incorrect Calculation

(l) Insufficient Random Values Usage

13.7.8.2. The Contractor shall furnish the code review test report to the School within SEVEN (7) days from the completion of the test and rectify any vulnerabilities or irregularities highlighted by the scanning tools, at no cost to the School. The Contractor shall re-scan the source codes after the rectification and provide the final test report to School for acceptance.

13.7.9. Code Review by Test Consultant

13.7.9.1. The Test Consultant shall provide an industry recognised static code analysis tool, which they own, to check and identify known errors, vulnerabilities and

weaknesses on all Application Software (including mobile codes or applications such as browser plug-ins, client-side scripts, applets, smart phone apps, etc.) developed at no additional cost to the School.

- 13.7.9.2. The static code analysis tool shall minimally perform the following:
- (a) Automated detection of Open Web Application Security Project (OWASP) Top 10 web application security risks;
 - (b) Highlight source code areas that poses security vulnerabilities; and
 - (c) Recommend remediation actions for security vulnerabilities.
- 13.7.9.3. The Test Consultant shall minimally perform one round of static code analysis on the quality of the System codebase using industry recognised software code analysis tools. The emphasis of the code review shall focus on quality which includes proper error handling, etc. The actual scope shall be proposed by the Test Consultant, subject to the School's approval.
- 13.7.9.4. The Test Consultant shall provide a review and recommendations of changes or fixes, to be submitted as a report to both the Contractor and the School. The Test Consultant shall also present the findings to the School in a face-to-face meeting(s). All security findings shall be resolved by the Contractor at no cost to the School.
- 13.7.9.5. The Contractor shall rectify all defects discovered by the third-party vendor at no cost to the School. The Contractor shall make all the necessary changes as recommended by the Test Consultant, unless an adequate justification or alternative is offered for each non-compliance and is approved by the School.

13.8. Test Type: Compliance Test

- 13.8.1. The Test Consultant shall conduct Compliance Test on the System to confirm that the System complies with the required regulatory standards, which includes:
- (a) Digital Service Standards (DSS)
 - (b) Achieve a score for each web page of at least 90% for both Accessibility and SEO measured by the Google Lighthouse or equivalent tool and the average page load time shall be within 3 seconds. The criteria are applicable to both Desktop and Mobile view
- 13.8.2. The Contractor shall rectify any non-compliance at no cost to the School.

13.9. Test Type: Usability Test

- 13.9.1. The Contractor shall perform Usability Test on the System to determine the usability of the System and rectify any usability issues at no cost to the School.

- 13.9.2. The Usability Test shall be conducted with actual users of the System or members of the public (if the System is a public facing application).
- 13.9.3. The School shall determine the medium on which the Usability Test will be conducted during the Requirements phase. The Usability Test shall be conducted on either of the following mediums:
- (a) A near finalised (UAT) version of the System; or
 - (b) On wireframe HTML mock-ups provided by the Contractor.
- 13.9.4. The Usability Test shall include tracking of the users' feedback on the usability of the System.
- 13.9.5. The Contractor shall provide a Usability Test Report at the end of the Usability Test, which minimally includes details like the following:
- (a) Number of users who participated in the test;
 - (b) Profile of the users who participated in the test;
 - (c) Summary of the feedback from the users; and
 - (d) Usability issues identified in the course of the test.
- 13.9.6. The Contractor shall rectify all major usability issues identified in the Usability Test in a suitable timeframe mutually agreed by the Contractor and the School, at no cost to the School.
- 13.10. Test Type: Functional Tests**
- 13.10.1. Functional Tests refers to tests carried out to ensure that a function behaves or performs in accordance with the functional specifications in these Requirements Specification.
- 13.10.2. The Functional Test is carried out from the perspective of the intended users and may include interaction with a website or a web portal leading to the actual application. The Functional Test may cover usability and design consistency.
- 13.10.3. As a function may require a collection of components (e.g. infrastructure, software and application code), the Contractor shall, at its own cost, ensure that related components are set up, tested and available for the Functional Test to be carried out.
- 13.10.4. For each function, the Contractor shall ensure that there are comprehensive test scenarios and test cases, including positive and negative scenarios, and time sensitive test cases (e.g. cross over year, leap year, and business calendar).
- 13.10.5. The Functional Test shall include use cases from different user perspectives, e.g.

- (a) Usage by School's end-users e.g. for submission of permit application,
- (b) Usage by Administrators e.g. management of business rules and testing of business rules before implementation into production, reports.
- (c) Usage by non-business users such as Contractor's application teams, System administrators and operators.
- (d) Usage of product-specific or bespoke functions of the System.

13.11. Test Type: Data Conversion & Migration Test

- 13.11.1. If data conversion or data migration is required in the project, details of the testing shall be included in the Master Test Plan.
- 13.11.2. Data Conversion & Migration Test shall include more than ONE (1) cycle of tests to ensure no data is lost during the actual data conversion/migration.
- 13.11.3. Data Conversion & Migration Test shall include the verification of the data before and after conversion/migration. All verification results shall be documented in the Data Conversion & Migration Test.

13.12. Test Type: Integration Tests

- 13.12.1. Integration Tests shall include the following:
 - (a) System Tests
 - (b) Interface Tests
- 13.12.2. System Tests
 - 13.12.2.1. The Contractor shall test the System and its interfaces from end-to-end. The Contractor shall ensure that the test scenarios cover the respective modules and functions within the System including interfaces with other systems.
 - 13.12.2.2. The Contractor shall ensure that System Tests include the following type of tests:
 - (a) Correctness
To ensure that data entered, processed and generated by the System is accurate and complete.
 - (b) Authorisation
To ensure that data is processed in compliance with the Security Clauses in **Clause 12.14.**
 - (c) Audit Trail

To test the System's capability to substantiate data processing that has occurred.

(d) Continuity of data processing

To test the System's ability to continue data processing when a problem occurs (where applicable).

(e) Service Levels

To ensure that the desired results of data processing will meet the service level requirements specified in **Clause 5.5**.

(f) Access Control

To ensure that System resources will be protected against accidental and intentional modification, destruction, misuse and disclosure.

(g) Reliability

To ensure that the System will perform its intended functions with the required precision over an extended period of time.

(h) Ease of Use

To ascertain the extent of effort required to learn, operate, prepare inputs for and interpret output from the System.

(i) Portability

To ascertain the extent of effort required to transfer software from one hardware configuration and/or System software environment to another.

(j) Coupling

To ascertain the extent of effort required to interface the System with all systems in the processing environment which either it receives or transmits data.

(k) Efficiency

To ascertain the amount of computing resources and code required by the System to perform its stated functions, e.g. java heap size usage, garbage collection efficiency, data source connection pool efficiency.

(l) Ease of Operations

To ascertain the extent of effort required to integrate the System into the operating environment and to operate the application system, including on-boarding of new modules or external systems into the System, helpdesk support, troubleshooting and problem resolution including integration to the operations management solution, distributed system management solution to alert, respond and whenever possible autocorrect. The Contractor shall involve the operations team in the design and management of the System.

- 13.12.2.3. The Contractor shall document the System Tests in a System Test package for the School's approval. The System Test package shall cover:
- (m) test objectives;
 - (n) comprehensive scenarios for each test objective;
 - (o) comprehensive test case for each test scenario;
 - (p) results of System Tests; and
 - (q) rectification works carried out.
- 13.12.2.4. The School reserves the rights to request the Contractor to make improvements or add test scenarios and to observe the System Test being carried out.
- 13.12.3. Interface Tests
- 13.12.3.1. The Contractor shall be fully responsible for working with and assisting all external parties in end-to-end interface testing, to ensure the timely and successful completion of acceptance testing for all interfaces.
- 13.12.3.2. The purpose of the interface tests is to ensure that the data format, data content and data transfer frequency are performed as per Requirement Specifications.
- 13.12.3.3. The Contractor shall submit the updated Master Test Plan or Integration Test Plan to the School for approval at least FOUR (4) weeks before commencing the interface tests.
- 13.12.3.4. The Contractor shall propose the schedule, including the detailed activities required for the full scope of interface acceptance testing. The detailed activities shall, amongst other things, include the required communication activities, email and/or briefing to these external parties and liaison with any other School agencies for the required connectivity to be open for the interface testing. The Contractor shall carry out the interface tests at the Contractor's own development environment to ensure that the data format, data content and data transfer frequency are as per Requirements Specification.
- 13.12.3.5. The interface tests shall include the following:

- (a) Connectivity testing;
- (b) Concurrent user accessibility testing;
- (c) Scenario testing: Ensuring that the interfacing systems are able to correctly handle and respond to both normal and exceptional file exchange/ processing scenarios; and
- (d) Full system integration testing: the System shall be able to fully simulate the actual operational interfaces.

13.12.3.6. The communication activities shall be planned sufficiently in advance so as to allow the external agencies to have adequate time for their own planning and preparation to meet the interface testing schedule.

13.12.3.7. The Contractor shall be required to work with the system interface parties and their Contractors to define the scope of the interface tests and the schedule. Each type of interface test may also involve several iterations.

13.12.3.8. The Contractor shall submit the Interface Acceptance Test Report to the School within SEVEN (7) days of the successful completion of the interface tests.

13.12.3.9. If the test is unsuccessful, or the School considers the test results to be unsatisfactory, the Contractor shall follow-up to make the necessary changes and re-perform the interface tests.

13.13. Test Type: Performance Test

13.13.1. The Contractor shall note that the purpose of the Performance Tests is to demonstrate that the proposed System meets the Requirement Specifications on the performance of the System specified in **Clause 5.5**.

13.13.2. After the SaaS System has been fully configured, the School shall load into the System test data which in the reasonable opinion of the School is suitable for testing whether the System is in accordance with the Requirement Specification, and with the advice and assistance of the Contractor, operate the System for a mutually agreed period to:

- (a) perform the School's routine transactions;
- (b) perform the transactions performed during any benchmark tests or other vendor demonstrations included, referenced, or incorporated in the Requirement Specifications;
- (c) carry out system functions test to determine whether the System meets the specifications, performs the functions, and meet the criteria for System Availability, response time and workload requirements set forth in the Requirement Specifications;

- (d) determine whether the documentation for the System meets the requirements of this Contract;
 - (e) perform such other transactions as may be necessary to test the System performance specified in the Requirements Specification.
- 13.13.3. Subject to the School's approval, the Contractor shall carry out the performance testing as well as application tuning to optimise the application performance in the System Performance Test environment.
- 13.13.4. The Contractor shall notify and obtain the School's approval on the recommended testing tools and number of software licences.
- 13.13.5. The Contractor shall be responsible for setting up the System Performance Test environment at its own cost, preparing all the data required for the System Performance Tests, refreshing the data where required, plan, execute and monitor all related batch job runs and other necessary work required by the System Performance Tests even if the System Performance Tests scope is not awarded to the Contractor.
- 13.13.6. The Contractor shall note that the System Performance Tests comprises the following:
 - (a) Benchmark Test;
 - (b) Stress Test;
 - (c) Performance and response time of API calls (if used); and
 - (d) Endurance Test.
- 13.13.7. The Benchmark Test shall validate system performance with the peak concurrent load factor (ONE HUNDRED percent (100%) of peak concurrent load factor) and normal think-times. The School shall confirm the normal think-times during the requirements phase.
- 13.13.8. The Stress Test shall validate system performance with peak concurrent load factor (ONE HUNDRED percent (100%) of peak concurrent load factor) and FIFTY percent (50%) the think-times defined in the Benchmark Test.
- 13.13.9. The Endurance Test shall establish system consistency over prolonged sustained peak concurrent load factor.
- 13.13.10. The updated Master Test Plan or detailed Performance Test Plan shall be reviewed and approved by the School.

- 13.13.11. The Test Consultant shall update the Master Test Plan or provide a separate Performance Test Plan using the School's Performance Test Plan template which documents minimally the background i.e. system overview, objectives, roles and responsibilities of the project team, testing methodology, key business processes, measurement of success, areas required for refinement and fine-tuning recommendations. The School's Performance Test Plan template will be provided to Contractor upon Contract award.
- 13.13.12. The Test Consultant shall propose in the Master Test Plan or Performance Test Plan how to generate the transaction load to test the System as though it were operating under live conditions, such as similar data size, usage scenarios, user base. The Test Consultant's Performance Test shall be carried out by the Test Consultant and the results of the test will be verified by the users.
- 13.13.13. The Test Consultant shall note that the Performance Test parameters shall be established according to the available resource in the Performance Test environment. The Contractor shall provide the results to the School to show that the application meets the performance targets for the System sizing proposed.
- 13.13.14. The Contractor shall submit the updated Master Test Plan or Performance Test Plan to the School for review and approval not later than ONE (1) month before the commencement of the System Performance Test.
- 13.13.15. The Test Consultant shall generate sufficient test coverage and a realistic amount of load together with batch processing on the application and system under test. The proposed test coverage and suggested amount of test data to be generated is subject to the School's review and approval.
- 13.13.16. The test coverage, the type of testing services and the amount of load generated on the system and application, which is subject to the School's approval, are dependent on the business requirements of the System, the System application architecture, the size of the user base, the number of concurrent users, the number of concurrent access, the number of concurrent requests, the system configurations, etc.
- 13.13.17. The performance of the System shall be baselined under the required load for user base and concurrent users within the specified System Response Time.
- 13.13.18. The Contractor shall ensure that performance testing shall be conducted in conjunction with applications' tuning to optimise the System performance in the Performance Test environment, regardless of whether the Performance Test are performed onsite or offsite.
- 13.13.19. The Contractor shall ensure that the performance testing shall be conducted without impact to other applications, implementation schedule or resource requirements by executing the test in different mix of scenarios such as low load vs high load, off peak periods and scheduling such that the environment be shared and mitigate any impact or the test result.

- 13.13.20. Upon completion of the Performance Tests, the Contractor shall submit and present the Performance Test Report to the School for review and approval. The Performance Test Report shall document test cases with results (expected and actual), statistics as evidence that performance tests have been carried out and the Systems are ready for review by the School, problems identified and recommendations for the application and system fine-tuning.
- 13.13.21. The School shall review and confirm if, based on the results of the Benchmark Test, Stress Test and Endurance Test, the System meets the performance requirements in the Requirement Specifications, and if not, whether the corrective actions to be undertaken by the Contractor to meet the requirements are acceptable to the School.
- 13.13.22. If the System is unable to meet the performance standards required by School, resulting in the need to conduct additional rounds of Performance Tests, the Contractor shall bear all the costs and expenses incurred for the additional resources needed, to conduct the additional round(s) of Performance Tests, including additional hardware and software.
- 13.13.23. In the event of non-compatibilities or System degradation during or as a result of the Performance Tests, the Contractor shall propose and implement solution(s) such as adding System resources to meet the System's requirements as approved by the School. The Contractor shall bear all the costs and expenses incurred to implement the solution(s).
- 13.13.24. The System shall be deemed to fail the System Performance Tests if:
- (a) it fails to provide any facility, transaction or function specified in the Requirement Specifications; or
 - (b) it fails to meet the System Response Time (as specified in Clause 5.5) for the Stress Test.
- 13.13.25. If the System fails to pass the System Performance Tests then the School may, by written notice to the Contractor elect at its sole option:
- (a) to have the Contractor provide a solution and to fix (without prejudice to its other rights and remedies) a new date for carrying out further tests on the System on the same terms and conditions (save that all costs which the School may incur as a result of carrying out such tests shall be reimbursed by the Contractor). Unless otherwise agreed in writing between the Parties, all such further tests shall not be construed as any grant of extension of time by the School and the Contractor remains liable for any delay in complying with its obligations under the Contract; or
 - (b) to accept the System subject to an abatement of the Contract Price such abatement to be such amount, as taking into account the circumstances, is reasonable. In the absence of written agreement as to abatement within fourteen (14) days after the date of such notice the School shall be entitled to exercise Sub-Clause (c) below; or

- (c) to treat the Contractor as being in breach of Contract and to reject the System as not being in conformity with the Contract in which event the School shall be entitled to terminate this Contract (without prejudice to the School's other rights and remedies) in accordance with **Clause 50 of Part 1 Section B**.

13.14. Test Type: Operational Readiness Test

13.14.1. The Operational Readiness Test shall include the following:

- (a) Installation Test;
- (b) System Failover and Recovery Test;
- (c) Backup and Restoration Test;
- (d) Compatibility/Portability Test; and
- (e) Disaster Recovery Test.

13.14.2. System Failover and Recovery Test

13.14.2.1. The System shall be designed to meet the System Availability requirements specified in the Requirement Specifications. The Contractor shall carry out failover test cases to ensure that there is no single point of failure for any components within areas such as infrastructure, software, and application.

13.14.2.2. The Contractor shall comply and conduct the failover test without any degradation of service or impact to System availability, and in adherence to the Requirement Specifications.

13.14.2.3. The Contractor shall carry out the failover test in a systematic way starting with individual areas such as network, hardware, software and application components such as shared libraries and application systems.

13.14.2.4. The Contractor shall also carry out the recovery tests to ensure that the System is able to recover from crashes, hardware failures and other similar problems. The Contractor shall simulate failure in areas similar to the failover test and restart the System to ensure that the System has successfully recovered from the failure.

13.14.3. Backup and Restoration Test

13.14.3.1. The Contractor shall perform Backup and Restoration Test to ensure that all backup media and procedures are working, and all backups can be restored properly.

13.14.3.2. The Backup and Restoration Test shall include all backup media and mechanisms in the System.

- 13.14.3.3. The Contractor shall provide a Backup and Restoration Test Report to the School after the test. The report shall include the results of the tests on the various backup media and mechanisms.
- 13.14.4. Compatibility/Portability Test
- 13.14.4.1. The Contractor shall carry out Compatibility/Portability Test to ensure that the System is accessible from the various different browser types.
- 13.14.4.2. The Contractor can use the following methods to facilitate the test:
- (a) Using a tool such as browser stack; or
 - (b) Using Virtual Machines with the appropriate browsers.
- 13.14.4.3. The Contractor shall rectify any major issues identified in the Compatibility/Portability Test in a mutually agreed timeframe, at no additional cost to the School.
- 13.14.4.4. The Contractor shall ensure the System is mobile optimised, across the various platforms (i.e. iOS, Android and Windows), especially for internet-facing applications.
- 13.14.5. Disaster Recovery Test
- 13.14.5.1. The Contractor shall carry out Disaster Recovery Test before System Commissioning to validate that the Disaster Recovery environment is working within expected parameters.
- 13.14.5.2. The Disaster Recovery Test shall simulate the network swing over from the Primary Data Centre to the DR Data Centre.
- 13.14.5.3. The Contractor shall provide a Disaster Recovery Test Plan to the School, detailing the objectives, activities and measurement metrics for the Disaster Recovery Test. The Disaster Recovery Test Plan shall be based on the activities described in the Disaster Recovery Plan.
- 13.14.5.4. The Disaster Recovery Test shall demonstrate that the requirements for Recovery Point Objective (RPO) and Recovery Time Objective (RTO) can be met.
- 13.14.5.5. The Contractor shall submit a Disaster Recovery Test Report to the School after the test for sign-off.

14. PROJECT MANAGEMENT AND QUALITY ASSURANCE**14.1. Project Organisation**

- 14.1.1. The Contractor shall submit a detailed project structure clearly defining the duties and responsibilities of all the personnel assigned to the project by the Contractor to the School for approval in the Project Management Plan.
- 14.1.2. The Contractor shall use or employ in and about the execution of the Contract only such persons as are careful, skilled and experienced in their respective vocations, trades and callings. The School shall be at liberty to object to and require the Contractor to remove immediately any such person employed by the Contractor in or about the execution of the Contract who in the sole opinion of the School misconducts himself or is incompetent or negligent in the proper performance of his duties and whose continued presence is undesirable or unacceptable. Such persons shall not be again used or employed in the performance of this Contract without the prior written permission of the School.
- 14.1.3. The Contractor shall ensure that the personnel assigned are technically competent and have good working knowledge of the hardware and software tools and platforms used for the application systems.
- 14.1.4. The Project Manager must be a Singapore Citizen or Singapore Permanent Resident except with the written agreement of the School.
- 14.1.5. The Contractor's Project Team shall have at least **TWO (2) years** of relevant technical expertise and working experience to deliver the system Development/Maintenance and Support services.
- 14.1.6. The Contractor's Project Manager is required to have at least **THREE (3) years** of good project management, supervisory skills and possess excellent communication skills. He should preferably be a university graduate with PMI or CITPM certification and have experience in managing IT projects of comparable magnitude and complexity.
- 14.1.7. The Contractor shall ensure that all personnel assigned to the project during the contract period have undergone Security Clearance. Personnel who have not received Security Clearance shall not be allowed to work on this project. As a guide, Security Clearance for Singaporean will require at least **FOUR (4) weeks** while that of foreigners require at least **EIGHT (8) weeks**. The Contractor shall take this into consideration in the event of any replacement of personnel. The School reserves the right to require that the Contractor's personnel undergo any further security clearance.
- 14.1.8. Upon acceptance by the School, each member of the Project Team shall be required to sign the "Non-disclosure undertaking" in the form provided in **Schedule 5 of Part 1 Section B** prior to the effective date of the Contract.

- 14.1.9. In the event that the Contractor's personnel who are carrying out the services cause any errors that negatively impact or disrupt services to users in any way whatsoever (whether due to insufficient testing conducted, lack of experience of the Contractor's personnel or any other reasons), the Contractor shall ensure that the errors are rectified immediately. Additional costs and man-days required by the Contractor to rectify the problem shall be borne entirely by the Contractor.
- 14.1.10. The Contractor shall monitor and manage effectively any sub-Contractor that has been selected in the discharge of their duties to meet the requirements established. All matters that require liaising between the sub-Contractors shall be coordinated by the Contractor to ensure harmony in the relationship among all parties concerned and to establish a common understanding of the School's requirements.
- 14.1.11. All sub-Contractors shall be subjected to the approval of the School.
- 14.1.12. A representative of the School shall be assigned throughout the duration of the project to manage the contract. He will monitor the progress of the project, conduct checkpoint reviews and ensure the timeliness and quality of the deliverables.

14.2. Role of Contractor's Project Manager

- 14.2.1. The Contractor shall designate a full-time Project Manager who shall be responsible for the overall management and co-ordination of the Contract.
- 14.2.2. The Contractor's Project Manager shall be the single point of contact to the School during the Contract Period.
- 14.2.3. The Project Manager shall be based in the Republic of Singapore from the commencement of the Contract to the expiry of the Performance Guarantee Period (PGP).
- 14.2.4. The Project Manager shall remain contactable to the School at all times. If the Project Manager is absent for any reason including annual, medical leave, away from Singapore for any duration, the Contractor shall ensure an Alternate Project Manager will cover his duties and functions.
- 14.2.5. The Alternate Project Manager shall be a person of equivalent or better qualification and experience and possess equivalent or higher School. He must have good knowledge of the progress status and issues relating to the Contract.
- 14.2.6. The Alternate Contractor's Project Manager shall be based in the Republic of Singapore during the period when the Project Manager is absent.
- 14.2.7. The Contractor shall provide in writing the particulars, qualification and experience of the Alternate Project Manager to obtain the School's prior approval. The appointment of the Alternate Project Manager (if any) shall be stated in the Project Management Plan submission.

- 14.2.8. The appointment of the Project Manager and other key personnel shall be subject to the School's approval. The Project Manager and key personnel shall not be absent from the project, unless otherwise approved by the School. The Contractor shall not change the designated Project Manager and key personnel as listed in their submission without the School's consent.
- 14.2.9. The Contractor's Project Manager must ensure that the deliverables are in accordance with the specifications stated in the Contract and the deliverables such as Service Requests are completed on schedule. He will undertake full responsibility for the quality of work produced by his team and the sub-Contractor. This includes ensuring that there is consistency and uniformity in the different work produced by his team and the sub-Contractors.
- 14.2.10. The Contractor's Project Manager will liaise between the School and his team members and shall report to the School periodically on the progress of the project. The frequency of the progress reporting shall be determined by the School.
- 14.2.11. Reviews of each milestone shall be incorporated at appropriate junctures throughout the course of the project. The Contractor is required to participate in all the reviews with the School at a location to be decided by the School. The Project Manager is expected to attend all reviews with the School. If the Project Manager is not available, he shall be duly represented by a person of higher School who shall have good knowledge of the project status and issues. This person shall preferably be from the committee which the Project Manager reports to. Such representations must be formally communicated to the School and must be agreed upon and confirmed by the School prior to the review meeting.
- 14.2.12. The School's Representatives may schedule progress meetings regularly. The Contractor's Project Manager is expected to be present at each progress meeting and report the progress on the execution of the Contract at the meeting. If the Project Manager is not available, he shall be duly represented by a person of higher School and who shall have good knowledge of the project status and issues. This person shall preferably be from the committee which the Project Manager reports to. Such representations must be formally communicated to the School and must be agreed upon and confirmed by the School prior to the progress meeting.
- 14.2.13. The Contractor's Project Manager shall be responsible for establishing the time and agenda for each progress meeting in view of the milestones achieved. The Contractor's Project Manager shall be prepared for each progress meeting with the necessary details for discussion. The Contractor's Project Manager shall highlight to the School's Representatives all required personnel from the School for the meeting. He shall also ensure that all relevant personnel from the Contractor shall be prepared for the meeting.

- 14.2.14. All minutes of progress meetings shall be produced by the Contractor's Project Manager and presented, within **THREE (3) working days**, to the School's Representatives for endorsement.
- 14.2.15. The Contractor's Project Manager shall also co-ordinate the various activities and meetings with the School and its existing relevant Contractors.
- 14.2.16. The Contractor's Project Manager shall maintain records of all meetings, functional specification reviews, development, user acceptance test and maintenance activities including proper accounting and administrative records of all services performed during the Contract Period.

14.3. Project Management Plan

- 14.3.1. The Contractor shall produce and maintain a detailed Project Management Plan (PMP) showing the proposed strategy and approach of the complete software life cycle and the dates of all identifiable activities and milestones necessary for the commissioning of the System. The Contractor shall take into consideration the deadlines stipulated by the School. The Project Management Plan shall be submitted on **TWO (2) calendar weeks** from the issuance of the Letter of Acceptance.
- 14.3.2. The Plan baseline shall be reviewed and endorsed by the School.
- 14.3.3. The Contractor shall update the Project Management Plan at interval of **TWO (2) calendar weeks** to reflect the planned and actual completion dates. The Plan shall be made available to the School for review.
- 14.3.4. The Project Management Plan shall include activities to be carried out by the School as well as all other personnel whose actions are required. The Project Management Plan shall include a diagram depicting the reporting structure and the key personnel who shall be involved in the project. It shall define clearly the Roles & Responsibilities of all personnel assigned by the Contractor to the Project.
- 14.3.5. The Project Management Plan shall include, at minimum, the following:
- (a) Project Scope, Objective, Goals and Approach;
 - (b) Project Description and Benefits;
 - (c) Project Organization including project team structure and roles and responsibilities of persons;
 - (d) Communications plan;
 - (e) Resource commitment (staffing, equipment, tools);
 - (f) Control and reporting including progress reporting and tracking, project meetings required, project approval and acceptance;

- (g) Implementation and delivery schedule including all project critical dates, milestones and activities;
- (h) Quality Management;
- (i) Resource Management;
- (j) Configuration/Change Management;
- (k) Risk Management;
- (l) Procurement Management;
- (m) Problem (issues, problems, defects) Management Framework; and
- (n) Project Deliverables.

14.4. Role of the Representative of the School

- 14.4.1. The representative of School shall endorse all minutes of meetings and proposed schedule of delivery produced by the contractor. He/she will validate that deliverables are of quality and to the School's satisfaction.
- 14.4.2. Upon attaining a milestone as defined in the project schedule, the appropriate work and deliverables must be signed off by the representative of the School after endorsement by the relevant approving committees. The sign-off shall signify that all requirements for that milestone have been met. The School shall reserve the right to withhold the sign-off until all works and deliverables meet the requirements.

14.5. Progress Reporting

- 14.5.1. The Contractor shall provide progress and status reports regularly to the School's Representatives. As a guide, the Contractor shall submit monthly progress report by the first week of the month during the contract period. The final format of the progress report will be submitted by the Contractor for approval by the School's Representative.
- 14.5.2. The progress report shall include the following:
 - (a) Achievements and deliverables;
 - (b) Action list;
 - (c) Updated project schedule versus baseline project schedule, including compliance and expected compliance with key milestones;
 - (d) All tasks which are in progress or which were scheduled to begin or end that week/month;

- (e) Problems encountered/envisaged and the Contractor's recommendations;
- (f) Delay(s), if any, the reasons and impact;
- (g) Change(s), if any, to the project scope;
- (h) Change(s), if any, to the functional specification of the System and/or the schedule, with full details;
- (i) Summary of service requests raised, their respective status and progress;
- (j) Resource utilisation report, such as CPU usage, memory usage, hard disk capacity, bandwidth utilisation, etc to facilitate capacity planning;
- (k) Summary of system/application incident reports;
- (l) Summary of security alert reports that includes the following:
 - (i) Application exception reporting,
 - (ii) Security incidents reporting and management,
 - (iii) Security reviews and audits,
 - (iv) Any other security activities such as disaster recovery and business continuity plan testing.
- (m) Operation reports for security patch fixes and updates;
- (n) Service availability with the analysis of problems that have impacted the service availability during the month;
- (o) Risk management; and
- (p) Commercial issues such as claims and billing details.

14.5.3. The Contractor shall also produce ad-hoc progress reports when requested by the School's representative. The report shall cover all tasks which are in progress or which were scheduled to begin or end that month.

14.5.4. The Contractor's Project Manager shall be responsible for informing the School, as early as possible, of any impending slippage in delivery dates and any matters likely to impede the progress of the project. The Project Manager shall put forth the recommendations on the alternatives available.

14.6. Mobilisation / Replacement of Key Personnel

14.6.1. The Contractor shall note that Key Personnel refers to the Contractor's Project Manager, Lead Architect, Lead Systems Analysts, Lead Quality Assurance Officer and Lead Programmers.

- 14.6.2. The Contractor shall note that the replacement of key Contractor personnel (for example: the Project Manager) shall be permitted only after **ONE (1)** year from commencement of the Contract unless such replacement is due to staff attrition.
- 14.6.3. In the event of a need for replacement of key Contractor personnel, the Contractor shall seek approval from the School in writing at least **ONE (1) calendar month** prior to the date of replacement, indicating the personnel to be replaced, reasons for the replacement and particulars of the new personnel who will be assuming the responsibilities concerned. The proposed replacement personnel must be of equal or higher qualification and skill level of the personnel that is leaving. The School reserves the right to accept or reject the proposed replacement personnel.
- 14.6.4. The Contractor shall also prepare a detailed replacement/handover plan to be submitted to the School.
- 14.6.5. The Contractor must submit the name and particulars of the replacement personnel to the School. All personnel mobilised to work on this contract shall be approved by the School prior to his/her mobilisation. The School reserves the right to accept or reject the proposed replacement personnel. The Contractor shall source for alternate replacement personnel at no additional cost to the School.
- 14.6.6. The Contractor shall be responsible for training the successor to be technically competent to carry out the work. The replacement personnel must be available for at least **ONE (1) calendar month** for the existing personnel to train him and hand over his responsibilities and duties. The training shall be conducted concurrently with the ongoing normal maintenance support required of the Contractor without affecting the service level. The cost incurred for the provision of the replacement personnel during the handling over period shall be borne by the Contractor.
- 14.6.7. The Contractor shall ensure the transition period is transparent to the School and does not impede the continuity of the operations.
- 14.6.8. The Contractor's Project Manager must supply evidence to the representatives of the School that the project handover is duly completed before releasing the personnel.
- 14.6.9. The Contractor must strictly adhere to the Project Handover Procedure from Quality Management System (QMS) adopted by the School. Where alternatives are proposed by the Contractor, the alternative procedure must be approved by the School.
- 14.6.10. The scope of the handover plan in the Project Handover Procedure, for any types of handover, shall include the following:
- (a) Processes and procedures;
 - (b) Roles and responsibilities;

- (c) Schedule Plan; and
- (d) Outstanding requests/activities.

14.7. Quality Assurance

- 14.7.1. The Tenderer shall prepare a quality assurance (QA) plan for approval by the School to ensure that the System delivered is of high quality. The Contractor must execute the QA plan to the satisfaction of the School.
- 14.7.2. The QA plan shall define how the quality of the System would be assured. It shall provide the mechanisms to ensure that the project adheres to sound technical principles and established industry standards.
- 14.7.3. The QA plan shall cover, at minimum, the following areas:
 - (a) The quality assurance activities and procedures for carrying them out;
 - (b) The standards, practices and conventions to be applied to the project;
 - (c) Appropriate quality assurance process for defect management, change management, configuration management, etc. The Contractor shall also include the software tools and forms used to support version control of systems, defect and change tracking, and change management;
 - (d) Duties and responsibilities of project personnel pertaining to quality assurance; and
 - (e) Fault reporting control and progress.
- 14.7.4. The QA plan shall include, at minimum, the design of forms or certificates for the acceptance of the System at each delivery point.

14.8. Performance Indicator

- 14.8.1. The Contractor shall establish a mechanism to collect and analyse performance indicators (e.g. Service Request Service Level). The indicators may be proposed by the Contractor, subject to the approval of the School. The School may from time to time, introduce its own measurements for the Contractor to adopt.
- 14.8.2. In the event that the Contractor is unable to meet the stipulated service level, it shall be indicated in monthly progress reports and to propose corrective or preventive measures in the progress reports.

15. COMPLIANCE TO STANDARDS AND METHODOLOGY

15.1. Quality Management System (QMS)

- 15.1.1. The Contractor shall preferably be ISO 9001 (latest version) certified in the area of testing, enhancement, implementation, support and maintenance of application systems.
- 15.1.2. The Contractor shall supply a copy of the Contractor's valid ISO 9001 Certificate together with its Tender Proposal if the Contractor is an ISO 9001 certified company. The Contractor shall provide further relevant information of the ISO 9001 standards (including the Contractor's company manual on ISO 9001) during the tender evaluation if requested by the School. If the Contractor is not an ISO 9001 certified company, then the Contractor shall state so in his Tender Proposal.
- 15.1.3. If the Contractor is an ISO 9001 certified company, the following would be applicable:
- (a) The Contractor shall provide details of its QMS standards, procedures and methodology to the School. The School may in its sole discretion request that the Contractor adopt other best practices. The application of the exact standards and procedures shall be subject to the mutual agreement between the Contractor and the School;
 - (b) The Contractor shall refer to the School's QMS and state any deviation of its methodology from the products and processes of QMS;
 - (c) If there is any change to the adopted standards, this shall be subject to the mutual agreement between the Contractor and the School; and
 - (d) The School shall reserve the rights to use any of the Contractor's standards, methodology, procedures and approaches delivered under this Contract solely for the purpose of the School.
- 15.1.4. If the Contractor is not an ISO 9001 certified company, the following shall apply:
- (a) The Contractor shall comply with the School Quality Management System (QMS) procedures to ensure the necessary deliverables as follow:

Table 6: System Application Development & Maintenance Methodology (ADMM)

Role	ADMM Phase	Responsibility	Deliverables
User (Customer)	Project Initiation	Define purpose and scope of the project.	<ul style="list-style-type: none"> Project Plan
	Requirements Specification	Specify the requirements needed for the new system/modules	<ul style="list-style-type: none"> Endorse Requirement Specifications

Role	ADMM Phase	Responsibility	Deliverables
	Preliminary Design	Review Preliminary Design & Prototype of Contractor	
	Detailed Design	Review Detailed Design and Functional Specifications of Contractor	<ul style="list-style-type: none"> Endorse Design and Functional Specifications
	User Acceptance	<ul style="list-style-type: none"> Review and carry out test plan. Confirm that the new system is implemented according to requirements specified Attend training session by S/W vendors 	<ul style="list-style-type: none"> Endorse User Acceptance Test
	Implementation Support	Provide feedback on the System's performance	<ul style="list-style-type: none"> Sign-off System Acceptance form
Project Working Team (Customer)	Requirements Specification	Gather, tighten, refine and document requirements specifications from user	<ul style="list-style-type: none"> Requirements Specification Review Results
	Preliminary Design	Review Preliminary Design of Contractor	
	Detailed Design	Review Detailed Design and Functional Specifications of Contractor	<ul style="list-style-type: none"> Design and Functional Specifications Review Results
	System Integration Testing	Review system test plan and results	<ul style="list-style-type: none"> System Test Results Review Records
	User Acceptance	Oversee user acceptance testing and provide assistance to users and Contractor, where possible.	<ul style="list-style-type: none"> User Acceptance Test Plan Review Records
	Implementation Support	Oversee Contractor implementing the System and provide assistance where possible	
	Maintenance	Oversee contractual matters; review major change requests from users and liaise with Contractor.	
Contractor	Project Initiation	Prepare Project Management Plan	<ul style="list-style-type: none"> Project Management Plan
	Requirements Specification	Gather, analyse, refine and document requirements specification from users	<ul style="list-style-type: none"> Requirement Specifications
	Preliminary Design and Prototyping	Translate requirements specification into logical design	<ul style="list-style-type: none"> Preliminary Design Specifications Prototype
	Detailed Design	<ul style="list-style-type: none"> Construct the physical design Prepare Detailed Design Specifications and program specifications 	<ul style="list-style-type: none"> Design Specifications Functional Specification

Role	ADMM Phase	Responsibility	Deliverables
	System Configuration / Development	<ul style="list-style-type: none"> System configuration Code the programs and carry out unit test 	<ul style="list-style-type: none"> System configuration document Program Source Codes Unit Test Package
	Data Conversion & Migration	<ul style="list-style-type: none"> Prepare Data Conversion and Migration Plan Load data into database on server Conduct verification and reviews on the migrated data 	<ul style="list-style-type: none"> Data Conversion and Migration Plan Migration Result report
	System Integration Testing	<ul style="list-style-type: none"> Setup hardware/software environment Carry out system integration testing 	<ul style="list-style-type: none"> System Test Plan System Test Package System Test Reports
	User Acceptance	<ul style="list-style-type: none"> Train users Set up the acceptance test environment Assist users in the preparation of user acceptance test plan Provide technical assistance to users in carrying out the user acceptance testing Resolve problems encountered during acceptance testing 	<ul style="list-style-type: none"> Training Materials User Acceptance Test Plan User Acceptance Test Package User Acceptance Test Result Reports
	Implementation	<ul style="list-style-type: none"> Prepare User Manual Prepare Operations Manual Set up production environment Prepare production system for implementation Conduct training Prepare Communication Plan Prepare Parallel Run 	<ul style="list-style-type: none"> Communication Plan Capacity Plan User Manual Operation Manual System Configuration Manual
	Performance Guarantee Period Support	<ul style="list-style-type: none"> Prepare Project Completion Analysis Report Conduct system performance test 	<ul style="list-style-type: none"> Project Completion Analysis Report
	Maintenance	<ul style="list-style-type: none"> Provide maintenance support to users 	<ul style="list-style-type: none"> Maintenance Plan Maintenance Log Progress Report

- 15.1.5. The Contractor shall adhere to all new or current standards and procedures introduced to the QMS from time to time or review and align equivalent company-internal standards accordingly when the need arises.

16. TRAINING**16.1. Overview**

16.1.1. The Contractor shall provide training to meet the following objectives:

- (a) To enable the change in mindset and appreciation of new roles and responsibilities where appropriate;
- (b) To enable the users to operate and use the features delivered for the new System; and
- (c) To enable a transfer of technology from the Contractor Development Team to the Contractor Maintenance Team (second level support) on the new System so that they will be able to operate, support, maintain and enhance the system.

16.2. General Requirements

16.2.1. The Contractor shall conduct training sessions for all users before the commissioning of the System. The Contractor shall also conduct a lecture-based training for management in which will be defined by the School, if required. The training sessions could be hands on or hands off sessions as requested by the School.

16.2.2. The Contractor shall quote, as an option to procure, on demand training session(s) to be conducted during the warranty and maintenance phase of the System.

16.2.3. The training classes could be refresher (advance or novice) courses or introductory courses for new staff or administrators. The Contractor shall provide continuous training for the above as and when the different user group request for it, if required by the School. The Contractor shall state clearly the additional cost to be incurred for such training to be conducted as and when the need arises in the future.

16.2.4. The Contractor shall provide suitable and adequate customised training for staff nominated by the School to enable them to carry out smooth operation and management of the System.

16.2.5. The Contractor shall propose the trainers who will be conducting the training and provide the trainers' credentials for the School's approval prior to the commencement of training.

16.3. Specific Requirements

16.3.1. The training provided shall be customised to suit the following categories of users:

- (a) Executive management staff;
 - (b) End users;
 - (c) Administrators (user and system);
 - (d) Helpdesk staff; and
 - (e) Staff nominated by the School.
- 16.3.2. The Contractor shall provide a comprehensive training proposal which includes the following:
- (a) Timetable for each training class;
 - (b) Dialogue sessions to be held: overviews, objectives, instructors, timetables etc.;
 - (c) Methods of instructions;
 - (d) Materials to be given during each of the training / dialogue sessions; and
 - (e) Pre-requisites for the participants.
- 16.3.3. The training provided shall include training on all hardware, software, products and services included in the proposed System.
- 16.3.4. The School shall be entitled to accept part or all of the training courses proposed by the Contractor. The School may, in its absolute discretion, request the Contractor to modify any training course and/or replace any course instructor the School finds unsatisfactory. Upon receipt of such a request, the Contractor shall do all that is necessary to comply with the request at no additional cost to the School.
- 16.3.5. The Contractor shall quote an option to provide all necessary facilities, equipment as well as the premises for the training.
- 16.3.6. If the School requires the training to be held in its proposed premises, the Contractor shall make arrangements for the setup of the System at the School's proposed training premises for these training purposes. The School shall provide the training venue equipped with PC workstations to enable the Contractor to conduct the training proposed in the training proposal.
- 16.3.7. The maximum capacity of the training classroom at the School's premises is **FIFTEEN (15)** participants.
- 16.3.8. The Contractor shall be responsible for setting up the entire Training environment of the System. The Contractor shall ensure that the Training environment is set up on time for the training to commence as scheduled.

- 16.3.9. The medium of instruction and training document shall be in English. The Contractor shall provide each trainee with a complete set of training documents and materials for his retention. Training materials can be in the form of e-Learning, PowerPoint or video formats etc.
- 16.3.10. For every course conducted by the Contractor, a complete set of the instruction guides and training materials shall be made available to the School. The School shall approve the materials proposed and have the right to use these training materials to conduct in-house course for its personnel.
- 16.3.11. The Contractor shall update the training documents and materials in accordance with changes made to the System at no additional charges to the School.
- 16.3.12. The Contractor shall provide training for major software release changes at no additional cost for the period of warranty and maintenance if required by the School.

16.4. Feedback and Evaluation

- 16.4.1. The Contractor shall be responsible for administering all the training sessions, e.g. registrations of participants, class attendance sheets, training feedback forms collation etc.
- 16.4.2. The Contractor is required to obtain feedback after each training session. The feedback forms shall be distributed to all participants in all training sessions. These shall be collected and handed over to the School for review.
- 16.4.3. In the event where the feedback gathered on any training conducted by the Contractor is less than **EIGHTY PERCENT (80%)** with above average rating, the School has the right to request for a re-training at no additional cost to the School.
- 16.4.4. The instructors provided by the Contractor for the training shall be proficient in conducting training and are equipped with good communication skills. Training to the users shall be conducted in user-friendly terms and language.

16.5. Schedule

- 16.5.1. All training courses offered shall be completed before the implementation of the System and enhancements to the System, whenever requested by the School.

17. DOCUMENTATION**17.1. Overview**

- 17.1.1. The Contractor shall supply all necessary documentation to enable the School to operate the System.

17.2. General Requirements

- 17.2.1. All documentation shall be in good, simple and concise English using accepted technical terms and symbols. All documents, except for the standard documentation that accompanies the appropriate hardware and system software, shall be made available in hardcopy and CD for ready reference and subsequent maintenance. All such documents shall have comprehensive indexes to facilitate quick reference. For maintainability, all such documentation must be converted to the latest version of the documentation tool which is used, if so required by the School.
- 17.2.2. The Contractor shall propose appropriate tools such as MS Word, MS Excel, etc., for the preparation of the documentation. This shall be subject to the School's approval.
- 17.2.3. All documentation provided shall be of the same version of the software proposed. The Contractor shall provide any revised editions, supplementary materials or new publication relevant to the System and documentation on enhancements at no cost to the School.
- 17.2.4. Where necessary, the Contractor shall adopt and maintain graphical representation (e.g. flow chart, screen layouts instead of textual) in all system documents.
- 17.2.5. All documents produced by the Contractor in fulfilling this Contract, shall become the property of the School. The School reserves the right to reproduce, at no cost whatsoever, any documentation supplied with the System for its own use. Prior approval must be obtained from the School for any reproduction and distribution of documents produced by the Contractor under this Contract.
- 17.2.6. The Contractor shall be responsible for the provision of adequate and suitable documentation in respect of the System. All documentation shall be completed and delivered to the School within the specified project schedule and as a pre-requisite for payment. The Contractor shall ensure that the documentation is kept up-to-date at all times.
- 17.2.7. The Contractor shall provide satisfactory answers to any reasonable queries raised by the School concerning any information stated in the documentation.
- 17.2.8. All documentation formats shall be subjected to approval by the School.

- 17.2.9. Draft version of the documents should be reviewed and vetted by the School prior to their official release.
- 17.2.10. All documentation provided shall display the date of document release and the version number of the document release on its cover page.
- 17.2.11. All initial draft versions of documents submitted to the School for review acceptance shall begin at Version 0.1, followed by Version 0.2 onwards with increments of 0.1 at each version revision. Only signed-off versions or versions deemed accepted by the School shall be set at Version 1.0 as the baseline version.
- 17.2.12. Each page of the document shall have its classification type stamped or typewritten in the centre, top and bottom of the page.
- 17.2.13. The Contractor shall supply and deliver full documentation and training manuals on all aspects of the System including the following:
- (a) Project documentation;
 - (b) System Software documentation (if applicable); and
- 17.2.14. All documentation shall be completed and delivered to the School as a prerequisite to the system commissioning.
- 17.2.15. Documents are part of the deliverables and the System shall not be deemed to be completed until it has been accepted by the School. Each phase of the development lifecycle and the entire project must be clearly documented.
- 17.2.16. The Contractor shall provide any other additional documentation as and when required during the duration of the project.
- 17.2.17. The Contractor shall also provide documentation and manuals of third-party hardware, software and equipment.
- 17.2.18. The School shall provide templates of the documentations wherever applicable.

17.3. Specific Requirements

- 17.3.1. The documentation shall include the following:
- (a) Project Management Plan;
 - (b) Requirement Specifications;
 - (c) Functional Specifications;
 - (d) Change Management Procedure;
 - (e) Detailed Design Specifications;

- (f) Program Specifications;
- (g) Prototype Specifications (if applicable);
- (h) User Interface Standard Specifications;
- (i) Data Conversion and Migration Plan;
- (j) Data Conversion and Migration Specifications;
- (k) Data Conversion and Migration Test Scenarios/Cases;
- (l) Data Conversion and Migration Report;
- (m) Interface Specifications;
- (n) System Test Plan;
- (o) System Test Package;
- (p) System Test Report;
- (q) User Acceptance Test Plan;
- (r) User Acceptance Test Package / Test Cases;
- (s) User Acceptance Test Report;
- (t) Training Plan;
- (u) Training Package / Training Guide
- (v) User Manual / User Guide;
- (w) Performance and Load Test;
- (x) Implementation Plan;
- (y) Communication Plan;
- (z) Transition Plan;
- (aa) System Handover Plan;
- (bb) Exit Plan;
- (cc) System Support Plan and Procedures / Operations Manual;
- (dd) Problem Escalation and Resolution Management;
- (ee) Business Continuity & Contingency Plan;

- (ff) Disaster Recovery Plan;
- (gg) Disaster Recovery Test Plan;
- (hh) Disaster Recovery Test Package;
- (ii) Disaster Recovery Test Report;
- (jj) Performance Guarantee Period Report;
- (kk) Project Status Report;
- (ll) Project Meeting Minutes;
- (mm) Audit reports;
- (nn) Audit action, progress reports;
- (oo) Quality Assurance Plan;
- (pp) Baseline Capacity Plan; and
- (qq) Quality Review Records.

17.3.2. The Contractor shall provide and release the System's program listings and source codes to the School at no additional cost. In addition, the Contractor shall be prepared to propose alternatives that shall enable the School to carry out modifications.

17.3.3. The Contractor shall provide and maintain an updated list of Software Configuration Index (SCI) and Document Configuration index (DCI) adopted in the System after implementation and upgrades/enhancements.

17.3.4. The SCI shall include at least the System's Application and System Software list such as the Operating Systems, Database Management systems and Application Softwares, etc that are not part of the School's central infrastructure environment.

17.3.5. The DCI shall include documentation produced for the System.

17.4. Rights to Application and Documentation

17.4.1. With regard to any Software supplied under the Contract over which the Contractor or third parties hold title or other rights, the Contractor shall permit or procure for the School and all authorised users of the programs (as the case may require) the right to use and apply that Software free of additional charge (together with any modifications, improvements and developments thereof) in the operation of the programs and in the operation of other computers which are linked to the project.

- 17.4.2. The Contractor's obligation in this Contract shall extend (inter alia) to enabling the School to disclose (under conditions of confidentiality to be agreed) programs and documentation for a third party to undertake the performance of services for the School in respect of such programs and documentation.
- 17.4.3. The School reserves the right to customise the application system and documentation submitted under this Contract solely for its use. Throughout the term of this Contract including the System Warranty Period, the School has the right to use the application system for any purposes. Such use of the application system shall not relieve the Contractor of its liabilities and obligations.
- 17.4.4. The School shall have the right to use any of the Contractor's standards, methodology, procedures and approaches delivered under this Contract solely for the purpose of the School.

18. TRANSITION MANAGEMENT

18.1. Overview

- 18.1.1. The objective of a transition management plan is to ensure a smooth handover and migration of all transferrable assets owned by the School or authorized by businesses from the outgoing incumbent to the incoming Contractor maintaining the System.

18.2. General Requirements

- 18.2.1. The Contractor is advised that the purpose of the transition is to ensure and achieve a smooth hand over of responsibilities. The Contractor shall ensure that the entire transition phase is as transparent as possible to the School users, that is, the users shall not experience any disruption of Services.
- 18.2.2. The Contractor shall comply with any direction from the School for assistance in relation to any aspect of take-over/hand-over of the information systems resources, including without limitation, human and technical assistance and the furnishing of such reports or updates in such form as may be required by the School. The Contractor shall give all necessary assistance to facilitate continuity in the operations of the School which depend on successful maintenance of its information systems operations.

18.3. Phase-in Transition

- 18.3.1. The Phase-in transition period shall be at least **ONE (1) month** before the expiry of the existing maintenance contract. Upon award of the Contract, the Contractor shall co-operate with the relevant parties to ensure that the services to the School are not disrupted and that a smooth hand-over of services is effected, either to the School or such other party as may be nominated by the School. The Contractor shall take-over all items owned by the School from the outgoing incumbent including the following:
- (a) Assets (hardware, software, media, documentations, licenses, storage media etc.); and
 - (b) Full set of documents describing the School's configuration, asset records, operating environment, operating manuals, accounts & passwords, contact information etc.
- 18.3.2. The Contractor shall be briefed by the outgoing incumbent on the relevant operational requirements during the first **TWO (2) weeks** of the transition period. During this period, the Contractor shall observe the incumbent in performing the daily operations of the System, so as to familiarise themselves with the System's operational requirements.

- 18.3.3. In the last **TWO (2) weeks** of the existing maintenance contract, the Contractor shall perform the daily operations of the System, under the supervision of the outgoing incumbent who will still be accountable for the operation of the System. At the end of the transition period, the Contractor shall take over and be fully responsible and accountable for ensuring the smooth on-going operation of the System and deliver all required services according to the contractual requirements stipulated in the contract.

18.4. Phase-out Transition

- 18.4.1. In the event of expiry of the Contract or termination of services of the Contractor, the Parties shall co-operate to ensure that the services to the School are not disrupted and that a smooth hand-over of services is effected, either to the School or such other party as may be nominated by the School.
- 18.4.2. Upon termination of the Contract, the Contractor shall bear all expenses incurred, including expenses in relation to handing-over of or transitional arrangements for or relocation of any of the Services under the Contract.
- 18.4.3. The Contractor shall ensure that the existing team is appropriately staffed and the exit plan is executed in an orderly manner without impacting the System and with minimal disruption to the operations of the School.
- 18.4.4. The Contractor shall hand over the responsibilities of maintaining the System to a new Contractor appointed by the School upon the expiry or termination of the Contract.
- 18.4.5. The Contractor shall hand over all items owned by the School to the new Contractor including the following:
- (a) Assets (software, media, documentations, licenses, storage media etc.); and
 - (b) Full set of documents describing the School's configuration, asset records, operating environment, operating manuals, accounts & passwords, contact information etc.
- 18.4.6. The Contractor shall brief the new Contractor on the relevant operational requirement and allow the new Contractor to shadow during the transition period. However, the Contractor shall remain fully responsible and accountable for ensuring the smooth on-going operation of the System and deliver all required services according to the contractual requirements stipulated in the contract during the transition period.
- 18.4.7. The briefing with the new Contractor for the System shall be completed **ONE (1) month** before the expiry of the maintenance contract.
- 18.4.8. The briefing and trainings shall be conducted in Singapore and shall be conducted in English by the Contractor.

18.4.9. In the last **TWO (2) weeks** of the maintenance contract, the Contractor shall supervise the new Contractor and personnel designated by the School in performing the daily operations of the System.

18.5. Exit Plan

18.5.1. The Contractor shall propose and deliver an Exit Plan within **TWELVE (12) months** after the Commissioning Date after the award of the Contract. The Exit Plan and the detailed schedule shall be subjected to the approval of the School with the duration of the exit period minimally at least **THREE (3) months** to account for sufficient time for the Incoming Contractor to perform shadow and reverse shadow of relevant operational requirements.

18.5.2. The Exit Plan shall include, at minimum, the following:

- (a) Processes and procedures;
- (b) Roles and responsibilities;
- (c) Definition of major milestones;
- (d) Schedule for completing / hand-over of outstanding tasks;
- (e) Contact list of vendors providing support;
- (f) Security procedures;
- (g) Deliverables such as outstanding logs, list of tasks in progress;
- (h) System and Application documentation (schedule of updates);
- (i) Cost implication of handling any proprietary vendor's tools with respect to licensing;
- (j) Define the work-in-progress i.e. ongoing tasks, other pending tasks and problems that have not been resolved or followed up by the existing Contractor;
- (k) How School's staff or other Contractor appointed by the School will be phased in to take over the System;
- (l) Shadowing and Reverse Shadowing periods;
- (m) Destruction of data by the Contractor and its Third-Party Contractors (including any Sub-contractors); and
- (n) Retrieval of any assets that are provided to the Contractor and its Third-Party Contractors (including any Sub-contractors).

- (o) “Parallel run” period whereby all enquiries/problem calls will be directed to the School’s staff or succeeding Contractor while the incumbent Contractor is still around;
 - (p) Training for new incoming incumbent; and
 - (q) Commitment of the Contractor and support prior to exiting.
- 18.5.3. The Contractor shall monitor and update the School on the progress of the handover.
- 18.5.4. The Exit Plan shall be reviewed and updated at the end of each contract year as well as **THREE (3) months** before the end of the Contract.
- 18.5.5. The exit transition period shall be managed and supervised by the School.
- 18.5.6. The Contractor shall complete all outstanding tasks and activities required of the Contractor. For outstanding tasks that may extend beyond the Contract Period, the School shall decide if such tasks should be handed over to the new Contractor.
- 18.5.7. The Contractor shall be responsible to conduct a detailed hand-over, inclusive of briefing and training sessions, of the complete system to the School or the next Contractor. Any cost incurred during the period of hand-over will be borne by the Contractor. The hand-over shall be conducted concurrently with the ongoing support required of the Contractor without affecting the Service Levels.
- 18.5.8. The Contractor shall hand-over all necessary documentation of the infrastructure, hardware, database and application software and records of problem resolution required for the effective maintenance of the System.
- 18.5.9. The Contractor shall complete defect management and corrective maintenance for all defects discovered during the Contract Period before handing over to the new Contractor.
- 18.5.10. The Contractor shall also perform an end-of-contract baseline update, which shall contain all the changes to the Application Software that have been made during the maintenance contract. The Contractor shall in accordance with the requirements of configuration management ensure completeness and proper configuration management of this baseline and submit it to the School for auditing and acceptance.