

REQUEST FOR QUOTATION

Quote requested from:

SAMPLE

1 HELLO Way
#13-04 HELLO Tower
HONG KONG 144909
Telephone No: 1234 5678
Fax No: 1234 5678

Requested for Quote No: SAMUTT19/23

Date issued: <Refer to <Portal>>

Date Due: <Refer to <Portal>>

Requested by: Sample Text

Email: sample_email@gmail.com

To: Contractors listed under Category 1 for JKT(R)5555-I Application Development and Maintenance (ADM)

Dear Sir/Madam,

You are requested by the SAMPLE (SAM) to quote for the Application Maintenance and Support services of the Integrated Grant Management System (IGMS) in accordance to JKT(R)5555-I and to the Clauses in this RFQ.

Please provide a proposal and quote for the Application Maintenance and Support services of IGMS as detailed in this RFQ.

Your submission is required to include the following details (Refer to Clause 16 – Guidelines for Submission for detailed info):

Section 1: Price Schedule

Section 2: Statement of Compliance

Section 3: Contractor Information

Section 4: Proposal for Services

Section 5: Other Information

Further information can be provided as additional sections, appendices or annexes.

Your quotation/proposal must reach us through <Portal> not later than the closing date and time indicated on the <Portal> Notice.

Late or incomplete submissions will not be considered.

I/We offer to supply the services specified in the RFQ; at the fees and charges offered according to JKT(R)5555-I; and on the same terms and conditions detailed in the agreement according to JKT(R)5555-I and to the Clauses in this RFQ.

Contractor's Name:

Address:

Signature _____

Dated this ____ day of ____ 2020

Contact name:

Phone:

Fax:

Email:

CONTENTS

1. 1. DEFINITION OF TERMSERROR! BOOKMARK NOT DEFINED.
 2. 2. INTRODUCTION AND IMPORTANT INFORMATION TO NOTEERROR!
BOOKMARK NOT DEFINED.
 3. 3. SCOPE OF RFQERROR! BOOKMARK NOT DEFINED.
 4. 4. SCOPE OF WORKERROR! BOOKMARK NOT DEFINED.
 5. 5. TECHNICAL AND FUNCTIONAL REQUIREMENTSERROR! BOOKMARK NOT
DEFINED.
 6. 6. APPLICATION SUPPORT & MAINTENANCE SERVICESERROR! BOOKMARK
NOT DEFINED.
 7. 7. CHANGE REQUESTSERROR! BOOKMARK NOT DEFINED.
 8. 8. END USER SUPPORTERROR! BOOKMARK NOT DEFINED.
 9. 9. TRAINING SESSIONS FOR IGMSERROR! BOOKMARK NOT DEFINED.
 10. 10. DATA MIGRATIONERROR! BOOKMARK NOT DEFINED.
 11. 11. SECURITY REVIEW AND TESTINGERROR! BOOKMARK NOT DEFINED.
 12. 12. OTHER GENERAL REQUIREMENTSERROR! BOOKMARK NOT DEFINED.
 13. 13. DOCUMENTATIONSERROR! BOOKMARK NOT DEFINED.
 14. 14. PAYMENT SCHEDULE AND BILLINGERROR! BOOKMARK NOT DEFINED.
 15. 15. VALIDITY OF RFQERROR! BOOKMARK NOT DEFINED.
 16. 16. GUIDELINES FOR SUBMISSIONERROR! BOOKMARK NOT DEFINED.
 17. 17. EVALUATION APPROACHERROR! BOOKMARK NOT DEFINED.
 18. 18. ENQUIRIESERROR! BOOKMARK NOT DEFINED.
 19. **ANNEX A** – DETAILED INFORMATION OF IGMSERROR! BOOKMARK NOT DEFINED.
 20. **ANNEX B** – GCC CUSTOMER HANDBOOKERROR! BOOKMARK NOT DEFINED.
 21. **ANNEX C** – CLAUSES IN EFFECT UPON EXPIRY OF JKT(R)5555-IERROR!
BOOKMARK NOT DEFINED.
 22. **ANNEX D** – OTHER SECURITY REQUIREMENTSERROR! BOOKMARK NOT DEFINED.
 23. **ANNEX I** – PRICE SCHEDULEERROR! BOOKMARK NOT DEFINED.
 24. **ANNEX II** – FORMAT FOR STATEMENT OF COMPLIANCEERROR! BOOKMARK
NOT DEFINED.
 25. **ANNEX III** – FORMAT FOR CONTRACTOR INFORMATIONERROR! BOOKMARK
NOT DEFINED.
 26. **ANNEX IV** – FORMAT FOR CONTRACTOR’S PERSONNEL
INFORMATIONERROR! BOOKMARK NOT DEFINED.
-

27. **ANNEX V – FORMAT FOR CUSTOMER REFERENCES** ERROR! BOOKMARK NOT DEFINED.

28. **SCOPE OF RFQ**

- 28.1. The terms and conditions of the quotation shall be in accordance to the Master Conditions of Contract of JKT(R)5555-I and this RFQ document. If there are any contradictions between the two, the Master Conditions of Contract shall prevail.

- 28.2. The scope of RFQ shall be as follows:

Mandatory Base Services

- A. **APPLICATION MAINTENANCE AND SUPPORT SERVICES FOR AN INITIAL PERIOD OF TWO (2) YEARS (YEAR 1 AND YEAR 2), FOR IGMS LISTED IN CLAUSE 5 AND ANNEX A;**
- B. **PROFESSIONAL SERVICES OF UP TO 500 MAN-DAYS PER YEAR, ON A PAY-PER-USE BASIS FOR ENHANCEMENTS OF IGMS IN YEAR 1 AND YEAR 2, WHERE UNUTILISED MAN-DAYS CAN BE ROLLED OVER TO THE SUBSEQUENT YEARS IF OPTIONAL SERVICES ARE AWARDED, AS SPECIFIED IN CLAUSE 7;**
- C. **PROFESSIONAL SERVICES FOR END USER SUPPORT OF UP TO 500 CASES PER MONTH, AS SPECIFIED IN CLAUSE 8;**
- D. **PROFESSIONAL SERVICES TO CONDUCT TRAINING FOR UP TO 300 MAN-DAYS PER YEAR FOR IGMS USERS, AS SPECIFIED IN CLAUSE 9; AND**
- E. **PROFESSIONAL SERVICES TO PERFORM DATA MIGRATION FOR UP TO 200 MAN-DAYS PER YEAR, AS SPECIFIED IN CLAUSE 10; AND**
- F. **PROFESSIONAL SERVICES FOR SECURITY SERVICES FOR UP TO 200 MAN-DAYS PER YEAR, AS SPECIFIED IN CLAUSE 11.**

Optional Services (Year 3 and Year 4)

- A. **APPLICATION MAINTENANCE AND SUPPORT SERVICES FOR IGMS FOR ANOTHER TWO (2) YEARS (YEAR 3 AND YEAR 4), LISTED IN CLAUSE 5 AND ANNEX A, SUBJECT TO YEARLY APPROVAL AND RENEWAL BY THE SAM;**
 - B. **PROFESSIONAL SERVICES OF UP TO 500 MAN-DAYS PER YEAR, ON A PAY-PER-USE BASIS FOR ENHANCEMENTS OF IGMS, AS SPECIFIED IN CLAUSE 7;**
-

- C. **PROFESSIONAL SERVICES FOR END USER SUPPORT OF UP TO 500 CASES PER MONTH, AS SPECIFIED IN CLAUSE 8;**
- D. **PROFESSIONAL SERVICES TO CONDUCT TRAINING FOR UP TO 300 MAN-DAYS PER YEAR FOR IGMS USERS, AS SPECIFIED IN CLAUSE 9;**
- E. **PROFESSIONAL SERVICES TO PERFORM DATA MIGRATION FOR UP TO 200 MAN-DAYS PER YEAR, AS SPECIFIED IN CLAUSE 10; AND**
- F. **PROFESSIONAL SERVICES FOR SECURITY SERVICES FOR UP TO 200 MAN-DAYS PER YEAR, AS SPECIFIED IN CLAUSE 11.**

- 28.3. Contractors shall quote and itemize clearly all the services (mandatory and optional) indicated in Clause 3.2 according to the format stated in Annex I. Any proposal to supply only parts of the above would be considered incomplete and deemed invalid.
 - 28.4. In addition to the requirements stated in Part 2 of IDA(T) 1432-G, the Awarded Contractor shall complete and fully take over the maintenance and support of IGMS within one (1) month from the award of the Letter of Acceptance (LOA) of this RFQ, or on a mutually agreed date with SAM.
 - 28.5. The Contractor shall note that there is a handover period which is estimated to last from four (4) weeks to eight (8) weeks before the Contractor's commencement in carrying out Year 1 of application maintenance and support in accordance with Clause 3.1.
 - 28.6. The Contractor shall co-operate with the incumbent contractor of maintenance services to ensure a smooth handover during this handover Period. The Contractor shall not be paid during this handover Period.
 - 28.7. As part of handover, the current incumbent will provide knowledge transfer and share how to use the onboarding checklist for each new agency, or new host institutions. The checklist shall be maintained regularly to ensure information is kept up-to-date.
 - 28.8. Upon award, the Contractor shall submit the takeover project schedule and include all the key milestones and deliverables in a Gantt chart, which is subjected to approval by SAM.
 - 28.9. SAM may terminate the support and maintenance services, at any time, by giving the Awarded Contractor one (1) month notice in writing without providing any reason. The charges to be made shall be pro-rated accordingly.
-

29. SCOPE OF WORKS

- 29.1. The Awarded Contractor shall provide Application Maintenance, Support Services and Enhancement Services in the form of service requests, and it shall cover all business functionalities and operations support of the system, including integration or interfaces with other systems with SAM and external systems from other Government agencies, where applicable.
- 29.2. In addition, the Awarded Contractor shall also assist with user account creation within IGMS for accounts such as Programme Manager, Agency Finance and RGO. This shall be done via service request, at no additional cost to SAM. The process would be further discussed between the Awarded Contractor and SAM.
- 29.3. The Awarded Contractor shall work closely with SAM's appointed personnel throughout the project.
- 29.4. SAM reserves the right to award the proposal in whole, in parts or not to award, regardless of whether it is mandatory base services or optional services in this RFQ.
- 29.5. The Contractor shall note that the projected maintenance commencement date of IGMS in Clause 3.4 is indicative. The Contractor shall note that the maintenance of the applications shall commence based on mutually agreed date between the Contractor and SAM.
- 29.6. SAM shall not be liable to compensate the Contractor as a result of change in maintenance commencement dates.

30. TECHNICAL AND FUNCTIONAL REQUIREMENTS

- 30.1. The IGMS consist of a) Landing Page Portal which is internet facing and built based on .Net and Sharepoint, and b) Backend Grant Administration System which is built based on Microsoft Dynamics AX 2012 R3.
- 30.2. The high-level IGMS functional specifications can found in Annex A.
- 30.3. IGMS will be hosted in Government Commercial Cloud (GCC) and Microsoft Azure by Oct 2020, based on a three-tier architecture. Please refer to Annex B for more information on the GCC environment. A copy of the architecture diagram of IGMS, the list of Azure resources and detailed information on external interfaces will be extended upon request. Without prejudice to Clause 4, information on the GCC, IGMS system architecture and external interfaces are subjected to change without prior notice to the Contractors during this RFQ period till the commencement date of the support and maintenance service.
-

30.4. IGMS shall be accessible using the latest client web browsers, which shall include but not limited to:

- Microsoft Internet Explorer;
- Google Chrome;
- Mozilla Firefox;
- Microsoft Edge; and
- Chromium.

30.5. The recommended browsers shall be reviewed from time to time. The Contractor shall be engaged to assess the compatibility of IGMS with the new browsers at no additional cost to SAM.

30.6. Monthly Account Review Exercise

30.6.1. THE AWARDED CONTRACTOR SHALL ASSIST TO GENERATE THE LIST OF ACCOUNTS ON A MONTHLY BASIS FOR AGENCY REPRESENTATIVES TO REVIEW.

30.6.2. THE CONTRACTOR CAN PROPOSE A MORE EFFICIENT PROCESS AND IS SUBJECTED TO SAM'S APPROVAL.

30.7. User Base and Support Cases

30.7.1. IGMS CURRENTLY HAS ABOUT 500 REGISTERED HOST INSTITUTIONS (INCLUDES PRIVATE COMPANIES), WITH ABOUT 48,000 FRONT END ACCOUNTS.

30.7.2. THE TABLE BELOW SHOWS THE ESTIMATED NUMBER OF INTERNAL USERS, VISITORSHIP PER MONTH AND THE SUPPORT CASES PER MONTH:

S/N	Description	Estimated Number of		
		AX users	Visitorship per day	Support Cases per month
1	IGMS Portal	-	400	200-300
2	IGMS AX	300	-	50-150

30.7.3. THE BELOW STATISTICS IS BASED ON RESOLVED CASES FROM JAN 2020 TO MAR 2020.

Type of Incident	Current Month (M = Mar 2020)	M-1	M-2
------------------	---------------------------------	-----	-----

User related issues			
Query/Request	277	201	403
Usage Errors	14	6	5
Technical related issues			
Data Related	13	10	12
Hardware and Network Problems	2	1	1
Programming Errors	10	13	4
Requirement Changes	7	4	6
System & Software Architecture Errors	1	11	0
Workflow related	3	0	0
Grand Total	327	246	431

30.8. External system interfaces with IGMS

30.8.1. IGMS IS CURRENTLY INTERFACED WITH THE EXTERNAL SYSTEMS SUCH AS:

S/N	External System	Purpose / How it is triggered
1	<AuthSystem>, Corpass and 2FA (Internet facing)	To authenticate prior to login to IGMS Real-time triggered by user's action.
2	MyInfo, EDH (Internet facing)	To retrieve and auto-populate personal data (MyInfo), and corporate related data (EDH) Real-time triggered by user's action.
3	<ResearchID> (Internet facing)	To link PI's <ResearchID> with IGMS Real-time triggered by user's action.
4	Elsevier Scopus and Expert Lookup (Internet facing)	To search for reviewers based on keywords Real-time triggered by user's action.
5	Application Mail Relay [AMR] (Intranet facing)	To send emails from SMTP relay (from Intranet) to SG Mail AMR. Batch job that runs on a daily schedule.
6	SAM Payment Module	For end to end payment processing of SAM claims

	(Intranet facing)	Batch job within IGMS that runs on a daily schedule.
7	A*STAR SAP (Intranet facing)	For payment processing of ASTAR claims Batch job within IGMS that runs on a daily schedule.

30.9. Future enhancements to IGMS

- 30.9.1. THIS SECTION DESCRIBES SOME POSSIBLE ENHANCEMENTS TO IGMS AND THESE WOULD BE RAISED TO THE AWARDED CONTRACTOR AS A CHANGE REQUEST UNDER CLAUSE 7.
- 30.9.2. THE CURRENT MIGRATION OF IGMS IS PERFORMED USING THE “LIFT AND SHIFT” APPROACH TO GCC. SAM IS KEEN TO INTRODUCE CI (CONTINUOUS INTEGRATION)/CD (CONTINUOUS DELIVERY) FOR AUTOMATION AND FASTER DELIVERY OF ENHANCEMENTS, WITH THE LANDING PAGE PORTAL PORTION (SHAREPOINT AND .NET) OF IGMS.
- 30.9.3. SAM IS ALSO LOOKING AT IMPLEMENTING A DATA PIPELINE TO ALLOW OTHER EXTERNAL SYSTEMS (E.G. GOVERNMENT, UNIVERSITIES, ETC.) TO EXTRACT INFORMATION OUT FROM IGMS, OR FOR OTHER EXTERNAL SYSTEMS TO POPULATE THE DATA INTO IGMS. THE TENTATIVE TIMELINE TO IMPLEMENT THIS IS BY JULY 2021 OR EARLIER. THERE ARE CURRENTLY ABOUT 200 TABLES IN IGMS, OF WHICH ABOUT 60 TABLES HAVE BEEN IDENTIFIED TO BE PART OF THE DATA PIPELINE FOR AGENCIES TO TAP ON. THE FREQUENCY OF DATA REFRESH SHALL BE CONFIGURABLE BY AGENCIES WHO WISH TO TAP ON THIS PIPELINE. THERE SHOULD ALSO BE DATA ACCESS SEGREGATION IN PLACE TO ENSURE USER WITH RELEVANT RIGHTS CAN EXTRACT OR INPUT DATA, TO AVOID ANY DATA COMPROMISE AND TO ACHIEVE DATA INTEGRITY.
- 30.9.4. THE CONTRACTOR SHALL INDICATE IN THEIR PROPOSAL, HOW THEY PLAN TO IMPLEMENT THIS DATA PIPELINE, WITH DETAILS SUCH AS HOW THEY WILL CONDUCT THE USER REQUIREMENT IN ORDER TO MEET THE BUSINESS OBJECTIVES.
- 30.9.5. SAM IS KEEN TO CONDUCT SERVICE JOURNEY WITH INTERNAL AND EXTERNAL STAKEHOLDERS TO IDENTIFY AREAS OF IMPROVEMENT, IN TERMS OF USABILITY AND IMPROVEMENT IN USER EXPERIENCE.
- 30.9.6. THE CONTRACTOR SHALL INDICATE IN THEIR PROPOSAL, HOW THEY PLAN TO EXECUTE THIS EXERCISE SO THAT USERS’ PAIN POINTS CAN BE CAPTURED, PRIORITISED AND ADDRESSED.
-

31. APPLICATION SUPPORT & MAINTENANCE SERVICES

- 31.1. The Awarded Contractor shall provide Application Maintenance and Support Services for IGMS covering the day-to-day production support and corrective, preventive maintenance. In addition, the Awarded Contractor shall adhere to all clauses indicated in Part 2, Section B, Clause 10 of JKT(R)5555-I and Annex C.
- 31.2. The Awarded Contractor shall carry out system maintenance activities, e.g. remedial, preventive, upgrades, in accordance to schedules agreed with the SAM.
- 31.3. The Awarded Contractor shall work with SAM's other relevant third-party vendors to ensure that these activities cause minimal interruption to SAM's operations.
- 31.4. There shall be a single point of contact for all maintenance and support related calls. The Awarded Contractor's Project Manager or equivalent who is the key personnel shall be contactable at all times via email, mobile phone or any given means of contact.
- 31.5. During system maintenance and support, the Contractor shall follow the Problem Management Procedure as indicated in Part 2, Section B, Clause 12 of JKT(R)5555-I and Annex C of this RFQ.
- 31.6. Maintenance Log and Progress Reporting
- 31.6.1. THE AWARDED CONTRACTOR SHALL MAINTAIN A LOG OF ALL MAINTENANCE ACTIVITIES, INCLUDING PREVENTIVE MAINTENANCE, CORRECTIVE MAINTENANCE AND OTHER SERVICES (MAINTENANCE LOG). FOR EACH ACTIVITY, THE LOG WILL RECORD AT LEAST THE DATE, TIME, DETAILS OF THE FAULT OR PROBLEM, CORRECTIVE AND FOLLOW-UP ACTION, AND THE SERVICE PERSONNEL. THE AWARDED CONTRACTOR SHALL PROPOSE A FORMAT OF THE MAINTENANCE LOG AND RECOMMEND PROCEDURES FOR ITS USAGE. THE FORMAT AND RECOMMENDED PROCEDURES FOR THE MAINTENANCE LOG SHALL BE SUBJECT TO SAM'S APPROVAL.
- 31.6.2. THE AWARDED CONTRACTOR SHALL SUBMIT A MONTHLY REPORT ON THE MAINTENANCE LOG, AND ALL RELEVANT MAINTENANCE ACTIVITIES PERFORMED IN THE PREVIOUS MONTH TO SAM WITHIN THE 10 WORKING DAYS OF THE NEW MONTH, UNLESS OTHERWISE AGREED BY SAM. THE FORMAT AND LEVEL OF DETAILS OF THE REPORT ARE SUBJECT TO THE APPROVAL OF SAM.
- 31.6.3. THE AWARDED CONTRACTOR MAY BE REQUIRED TO PRODUCE AD-HOC PROGRESS REPORTS WHEN REQUESTED BY SAM. THESE REPORTS SHALL
-

BE SUBMITTED WITHIN A STATED NUMBER OF DAYS MUTUALLY AGREED BETWEEN SAM AND THE AWARDED CONTRACTOR'S PROJECT MANAGER.

- 31.6.4. THE AWARDED CONTRACTOR SHALL BE REQUIRED TO INFORM SAM IMMEDIATELY OF ANY IMPENDING SLIPPAGE IN THE DELIVERY DATES AND ANY MATTERS LIKELY TO IMPEDE THE PROGRESS OF THE PROJECT. RECOMMENDATIONS SHALL BE PUT FORTH BY THE AWARDED CONTRACTOR'S PROJECT MANAGER ON THE BEST ALTERNATIVES AVAILABLE.

31.7. Handover of Maintenance Support

- 31.7.1. IN THE EVENT THAT THE MAINTENANCE CONTRACT IS TERMINATED OR EXPIRES, THE AWARDED CONTRACTOR SHALL FURNISH SAM WITH A DETAILED HANDOVER PLAN AND SCHEDULE AT LEAST ONE (1) MONTH PRIOR TO THE EFFECTIVE DATE OF THE TERMINATION OR EXPIRY. THE HANDOVER PLAN AND THE DETAILED SCHEDULE SHALL BE SUBJECT TO SAM'S PRIOR WRITTEN APPROVAL.
- 31.7.2. THE AWARDED CONTRACTOR SHALL BE RESPONSIBLE FOR CONDUCTING A DETAILED HANDOVER OF THE COMPLETE SYSTEM TO ANY THIRD PARTY APPOINTED BY SAM TO MAINTAIN IGMS DURING THE LAST TWO (2) MONTHS OF THE MAINTENANCE CONTRACT. THE HANDOVER SHALL BE CONDUCTED CONCURRENTLY WITH THE ONGOING NORMAL MAINTENANCE SUPPORT REQUIRED OF THE AWARDED CONTRACTOR WITHOUT AFFECTING THE MAINTENANCE SERVICE LEVEL.

31.8. Support Personnel

- 31.8.1. THE AWARDED CONTRACTOR SHALL STATE THE NUMBER OF STAFF (INCLUDING END USER SUPPORT PERSONNEL) TOGETHER WITH DETAILS OF THEIR QUALIFICATIONS AND EXPERIENCE WHO WILL BE GIVING SUPPORT FOR IGMS AS PER THE FORMAT PROVIDED IN ANNEX IV.
- 31.8.2. THE AWARDED CONTRACTOR SHALL NOTIFY SAM WITHIN SEVENTY-TWO (72) HOURS OF ANY CHANGES IN SUPPORT STAFF. IT SHALL BE THE AWARDED CONTRACTOR'S RESPONSIBILITY TO STAFF THE SYSTEM SUPPORT SERVICES WITH QUALIFIED PERSONNEL HAVING THE NECESSARY TECHNICAL AND COMMUNICATION SKILLS. THE SYSTEM SUPPORT PERSONNEL SHALL POSSESS AT LEAST THE FOLLOWING CHARACTERISTICS:
- Possess the relevant technical IT expertise and skills;
 - Be able to speak clear and good conversational English;
 - Good at problem solving.
-

31.8.3. THE PROJECT MANAGER AND TEAM PROPOSED BY THE CONTRACTOR MUST BE EXPERIENCED IN MANAGING PROJECTS OF SIMILAR SCALE AND NATURE COMPARED TO THE SCOPE OF WORK DEFINED IN CLAUSE 4.

31.9. The Awarded Contractor shall, at no additional cost to the Government, provide internet laptops, with software and licenses, for its staff to access GCC. The software and licences shall minimally include, Intune, MS AAD, etc. or any software as may be necessary to access GCC.

32. CHANGE REQUESTS

32.1. The Awarded Contractor shall adhere to all clauses stated in Part 2, Section B, Clause 8 of JKT(R)5555-I and Annex C, and provide professional services for changes to IGMS. Such requests shall be raised as change requests (CR), and the Awarded Contractor shall propose a standard man-day rate for CRs in the proposal.

32.2. The Change Request could be raised for the following purposes:

- a. Making changes to the System (as described in Clause 7);
- b. Conduct training (as described in Clause 9);
- c. Data migration (as described in Clause 10);
- d. Security Review and Testing (as described in Clause 11); and
- e. Any other changes as requested by SAM.

32.3. Classification and Service Levels for Change Requests:

- Major Change Request – Refers to change request that require more than 20 man-days to implement.
- Minor Change Request – Refers to change request that require less than or equal to 20 man-days to implement.

32.4. The Awarded Contractor shall submit a report on ‘Assessment of effort’ within two (2) calendar weeks for every major change request and within one (1) calendar week for every minor change request raised, or upon mutual agreement with SAM.

32.5. Depending on the estimated man-days required, the Awarded Contractor shall complete and implement all Change Requests within the specified turnaround time:

S/N	Estimated CR man-days effort	Service Level for CR Completion Time
-----	------------------------------	--------------------------------------

S/N	Estimated CR man-days effort	Service Level for CR Completion Time
1	Lesser than or equal to ten (10) man-days	Within 5 working days or mutually agreed timeline
2	Greater than ten (10) and lesser than twenty (20) man-days	Within 10 working days or mutually agreed timeline
3	Greater than or equal to twenty (20) man-days	Based on mutual agreed timeline

- 32.6. The Awarded Contractor shall implement all CRs approved by SAM.
- 32.7. The Awarded Contractor shall note that CRs implemented shall not incur additional maintenance charges unless it falls beyond the current maintenance scope of IGMS and is subjected to approval by SAM. Any proposal for additional maintenance charges shall be highlighted to SAM for discussion and mutual agreement.
- 32.8. The Awarded Contractor shall note that in case of change of request priority by the users or under any unforeseen circumstances, SAM reserves the right to re-prioritise change requests given earlier.
- 32.9. The Awarded Contractor is responsible for ensuring that the Change Request is successfully implemented according to agreed schedule based on agreed man-effort. If the Awarded Contractor cannot meet the pre-agreed schedule/man-efforts, any additional costs incurred shall be borne by the Awarded Contractor. It shall be the Awarded Contractor's responsibility to prioritise the change requests with agreement from the Customer.
- 32.10. The Awarded Contractor will be required to mobilise additional manpower and this manpower shall be available within seven (7) calendar days after being notified by SAM to undertake additional urgent requirements.
- 32.11. The Awarded Contractor shall note that the implementation of a change request may be on a one-time basis or in phases, to be specified by the Customer.
- 32.12. The CR would only be considered as completed after it has been successfully deployed to production environment and when all relevant documentation is prepared/updated and accepted by SAM. If there is delay caused by SAM, this delay will not be included in the computation of the Change Request Completion requirement.

33. **END USER SUPPORT**

- 33.1. The Contractor shall indicate the end user support methodology in their proposal, describing in detail, how they intend to implement the end user support, track and monitor the cases, based on the clauses described below.
- 33.2. The Awarded Contractor's Project Manager shall be appointed to be the primary contact point for End User Support services to address:
- (a) Account related issues (e.g. login issues, creation of accounts, etc.);
 - (b) Technical issues (e.g. browser issues, security issues, etc.);
 - (c) Queries on business policy by redirecting them to relevant parties;
 - (d) Usage issues (e.g. Guide on the correct use of the system, etc.); and
 - (e) Other user queries
- 33.3. With reference to Clause 5.7.2, the current number of enquires or issues raised (hereafter known as "case") are around 500 per month during peak season.
- 33.4. The Awarded Contractor shall note that for an enquiry or issue, there could be multiple follow up calls by internal users (e.g. agencies) or external users (e.g. researchers, host institutes, etc.) to the helpdesk. This should be treated as one (1) case.
- 33.5. The Awarded Contractor shall be required to work directly with the relevant parties (e.g. production support team/SAM representatives) to resolve issues and/or account provisioning.
- 33.6. The Awarded Contractor shall be required to meet with SAM representatives and address issues raised from calls and emails. The frequency of such meetings will be determined by SAM.
- 33.7. The End User Support team must be based in Hong Kong.
- 33.8. The Awarded Contractor shall provide a single point of contact for Users with a common contact number. SAM would provide government laptops and one government-domain email account to the Awarded Contractor for the purpose of providing end user support service. The Awarded Contractor shall return the laptops, in good working condition, to SAM upon the expiry or termination of this maintenance contract. The number of government laptops to be provided shall be mutually determined between the government and the Awarded Contractor.
- 33.9. The Support Hours are defined as follows:

Days of the week	Operational Hours
Monday to Friday	0830 hr to 1800 hr
Saturday, Sunday and Public Holidays	Nil

If New Year Eve or Chinese New Year Eve or Christmas Eve falls on a weekday	0830 hr to 1300 hr
--	--------------------

- 33.10. The Awarded Contractor shall provide an end user support plan, subjected to the SAM's approval. The end user support plan shall outline the following:
- (a) Contact Information of the support personnel;
 - (b) Service level for case closure (in terms of response times, problem resolution times); and
 - (c) Process for Problem reporting, analysis, escalation, resolution and closure.
- 33.11. The Awarded Contractor shall maintain all cases received and keep proper records on all enquires, problem reporting, escalation, tracking and resolution. A monthly report summarising the total of cases (both open/closed) and list of cases handled shall be submitted as part of the monthly progress report.
- 33.12. For users' queries and feedback via email, upon receipt of the email, the Awarded Contractor shall acknowledge the email immediately followed by a reply by next working day (could be an interim reply or status reporting) and a final reply within three (3) working days, if necessary.
- 33.13. The End User Support personnel shall track all incoming calls and emails including those that cannot be answered to immediately. A case shall not be closed until it has been attended to and closed by the user.
- 33.14. The End User Support personnel shall escalate the problems to the relevant parties for actions if required and track the status of the cases periodically until they are closed by the users.
- 33.15. The End User Support key personnel shall be contactable at all times during the operational hours as stated in Clause 8.9 and shall respond within thirty (30) minutes from the time it is lodged.
- 33.16. The Awarded Contractor shall maintain the following service level for case closure:
- (a) For cases logged that have direct impact on application, they shall be closed within two (2) calendar days; and
 - (b) For cases logged that are usage related, they shall be closed within three (3) working days.
- 33.17. As part of monthly reporting, the Awarded Contractor shall provide various reports to track and monitor the number of cases, service level, etc. Examples of reports are listed in the table below:
-

S/N	Type of report	Details
1	Case Log (i.e. telephone calls and emails)	Case ID; Caller information (Name, Agency (if relevant), email, other relevant contact info) Type of user group (e.g. Programme Officer, Reviewer, etc.) Date and time of Case reported; Type/Category of Case; Case description; Details of Case resolution; and Date and time of Case closure.
2	Call statistics report	Category and type of calls; Total no. of calls received; and Number and % of calls answered
3	Email statistics report	Category and type of email; Number and % of emails replied; Number and % of 1st instance email resolved within service level; and not within service level; Provide reasons for those that did not meet service level; and Number and % of emails replied within service level and not answered within service level (Provide reasons for those that did not meet service level).
4	Trending reports	Time based trending of types of issues reported and resolved Comparison of cases across past 3 months, or year-on-year.

- 33.18. The Awarded Contractor shall work with SAM to finalise the types of reports to be incorporated as part of the overall monthly progress report.
- 33.19. The Awarded Contractor shall note that the training to be conducted for the call agents prior to the commencement of the end user support is deemed to be included as part of the cost.
- 33.20. SAM will request the Awarded Contractor to conduct random satisfaction surveys to ensure quality of end user support. If the results are deemed unsatisfactory, the Awarded Contractor shall improve the quality of the end user support and provide progress updates on what had been done to address the gap. A post-action satisfaction survey shall be conducted by the Awarded Contractor, within 3 months of the execution of the improvement plan, to measure the satisfaction level among the users.

- 33.21. SAM reserves the right to request for changes in end user support personnel, when necessary. The Awarded Contractor shall provide a replacement within 2 months of notice from SAM.

34. TRAINING SESSIONS FOR IGMS

- 34.1. Upon request by SAM via Change Request, the Awarded Contractor shall provide training to users of IGMS during the Contract Period and comply to Part 2, Section B, Clause 7 of JKT(R)5555-I and Annex C.
- 34.2. Training shall be conducted through using presentation slides with screenshots and/or show-and-tell of how the system functions, followed by Question and Answer (Q&A) segment, to allow users to clarify any doubts. Each session shall be held at a maximum of 4 hours. For queries which cannot be answered during the session, the Awarded Contractor shall follow up with the user(s) till closure of the query.
- 34.3. The sessions can also be conducted on a smaller scale, for users who are already familiar with basic understanding of IGMS but require the Awarded Contractor's assistance to clarify specific queries, through consultative approach. Similarly, each session shall be held at a maximum of 4 hours.
- 34.4. The sessions could be based on selected modules or functions to suit different user roles (such as user administrator, programme manager, and finance officers) within IGMS.
- 34.5. The training could be conducted at the Customer's premises (up to 100 pax per session) or online (up to 200 pax per session), as determined by the customer. Users attending the training will be responsible for bringing their own laptops.
- 34.6. After each training session, the Awarded Contractor shall conduct user satisfaction survey with the participants and update the Customer on the survey results, and identify areas of improvement, where applicable. The survey questions shall be agreed by Customer and regularly reviewed to ensure the questions remain relevant.
- 34.7. The Awarded Contractor shall provide all the training materials such as presentation slides. Such materials shall be submitted to and approved by the SAM at least two (2) weeks before the commencement of the training. The medium of training and materials shall be in English.
- 34.8. SAM will provide the set of user guides and existing training materials which had been done up by the current incumbent. The Awarded Contractor shall maintain the materials and ensure the information is kept up-to-date in accordance with
-

changes to the System. The Customer shall own all the training materials, including the softcopy, developed under this Contract.

- 34.9. The Customer estimates that at least 10 sessions of training (of different modes as described in above Clauses 9.2 to 9.5) would be conducted per year. The Contractor shall quote for the effort to conduct training based on 300 man-days per year.

35. DATA MIGRATION

- 35.1. Upon request by SAM via Change Request, the Awarded Contractor shall provide data migration service to move requesting agency's existing data into IGMS, and the Awarded Contractor shall adhere to Part 2, Section B, Clause 9 of JKT(R)5555-I and Annex C.
- 35.2. A round of data migration has been done for each of the 4 funding agencies. This scope of work is only required if agencies request for their data to be migrated into IGMS.
- 35.3. The Awarded Contractor shall migrate, convert and upload the data from the requesting agency into IGMS. This includes the correct conversion of all indexes, coded fields (e.g. status codes), documents and any linked records.
- 35.4. As part of handover, the current incumbent will pass the data migration templates (54 templates for Pre-award and 58 templates for Post-award) to the Awarded Contractor. The Awarded Contractor shall ensure in-depth understanding on the use of these templates and counter propose to SAM if there is a more effective approach to conduct the data migration.
- 35.5. The Awarded Contractor shall specify the security precautions taken to safeguard the integrity of the data during the data migration exercise.
- 35.6. The Awarded Contractor shall be responsible for all activities required for data conversion. Where the activities require user involvement, the Awarded Contractor shall automate as far as possible all the preparation of the data prior to user involvement.
- 35.7. The Awarded Contractor shall ensure that the data migration or data extraction activities will not affect the daily operation of the new onboarding agencies.
- 35.8. The Awarded Contractor shall prepare and obtain approval from the Customer, for the data migration plan prior to the data migration, and ensure the data migration plan is updated till successful completion of the data migration.
- 35.9. The Awarded Contractor shall convert, transcribe and load data from database files of existing Systems of the requesting agency to the data format in IGMS.
-

- 35.10. The Awarded Contractor shall liaise directly with the current suppliers handling the maintenance of the requesting agencies' existing Systems and the FM teams to extract the data from the existing systems for the purpose of the data migration exercise and manage the entire process for data migration.
- 35.11. The Awarded Contractor shall be responsible and shall bear the cost to rectify any erroneous data if any inaccurate and incomplete data arise from any negligence or error on their part.
- 35.12. The Awarded Contractor shall also undertake the correction of all errors to the satisfaction of the Customer based on specified performance and acceptance standards. The Customer reserves the right to specify the performance standards and acceptance standards for the purpose of acceptance.
- 35.13. If there are data to be corrected as a result of the migration, the Awarded Contractor shall provide the means to correct these data. Access to such programs shall be controlled and appropriate report created to track the changes made.
- 35.14. The Awarded Contractor shall ensure that safeguards are put in place during the transcription/migration to maintain the physical security and physical integrity of any source records which are captured.

36. SECURITY REVIEW AND TESTING

- 36.1. Upon request by SAM via Change Request, the Awarded Contractor shall engage an independent and competent third-party security consultant to conduct security review and testing (including follow-up testing and review) of the System and processes, and to document the security findings and recommendations in a report. The choice of the third-party security consultant shall be subjected to the Government's approval. The Awarded Contractor shall provide the necessary resources to assist in the security review and testing, and to fix any findings, and to perform mitigations (when applicable) and follow-ups at no additional cost to the Government.
- 36.2. The scope of the security review and testing is expected to include the following:
- (a) System hardening and security configuration review of the entire System;
 - (b) Quarterly Vulnerability Assessment of the entire System (including network, servers, applications, services, and security components);
 - (c) Annual security source code review for the applications;
 - (d) Annual application penetration testing for vulnerabilities (e.g. listed under OWASP Top Ten) which include but not limited to:
 - i. Injection
 - ii. Cross Site Scripting (XSS)
 - iii. Broken Authentication and Session Management
 - iv. Insecure Direct Object References
-

- v. Cross Site Request Forgery (CSRF)
- vi. Security Mis-configuration
- vii. Insecure Cryptographic Storage
- viii. Failure to Restrict URL Access
- ix. Insufficient Transport Layer Protection (e.g enabling of weak cipher suite in the SSL protocol) Un-validated Redirects and Forwards
- x. Buffer overflows;
- xi. Improper Error and Exception handling;
- xii. Insecure access control mechanism (e.g account privilege escalation, failure to restrict URL access, etc);
- xiii. Malicious code injection (e.g SQL injection, cross-site scripting, etc);
- xiv. Cross-Frame Scripting (CFS);
- xv. Insecure authentication and session management;
- xvi. Security misconfiguration; and
- xvii. Application business logic flaws.

36.3. The Awarded Contractor shall take the following sets of security policies, standard, and guidelines into consideration in the security review:

(a) Government/Customer's security policies, standards and guidelines; and

(b) Industry security standards and best practices (e.g. ISO 27001/27002, Open Web Application Security Project's (OWASP) practices, vendor's hardening guidelines, Center for Internet Security hardening benchmarks, NIST security guidelines, Common Weakness Enumeration).

36.4. The security consultant performing the security review shall possess the necessary skills, knowledge and experience in security source code review practices based on industry standards such as OWASP, CERT.org Secure Coding Standards.

36.5. The Awarded Contractor shall be responsible to work with the Government and / or its appointed independent third-party in meeting the objectives of the review and testing.

36.6. The Awarded Contractor shall ensure that the security consultant performing the security review and testing documents all the security findings and the recommendations in the form of a report. The report shall be submitted to the Government for approval within two (2) weeks after completion of security review and testing, and the Awarded Contractor shall ensure that the approved recommendations are implemented through proper change management processes within four (4) weeks or within a schedule mutually agreed between the Government and the Awarded Contractor upon acceptance of the report at no additional cost to the Government.

- 36.7. Following the implementation of the recommendations, the Awarded Contractor shall ensure that the independent third-party security consultant performs a follow-up review and testing to ensure the findings are closed.
- 36.8. The Awarded Contractor shall work with the Government representatives to enable them to verify the findings and assess the recommendations in the report at no additional cost to the Government.
- 36.9. The Awarded Contractor shall be responsible to address the security findings identified in the third-party security review and testing to a level that is acceptable by the Government. The Awarded Contractor shall also bear all the cost of any retrofitting and rectification resulting from the security review and testing.
- 36.10. In the event that the Awarded Contractor fails the security review and testing, the Awarded Contractor shall engage security consultant to conduct the follow-up review and testing at no additional cost to the Government
- 36.11. Restoration Test
- 36.11.1. UPON REQUEST BY SAM VIA CHANGE REQUEST, THE CONTRACTOR SHALL CONDUCT SYSTEM OR/AND DATABASE RESTORATION TEST. THE CONTRACTOR SHALL:
- A. RESTORE SYSTEM FROM CLEAN BACKUPS;
 - B. REBUILD SYSTEM FROM SCRATCH
 - C. RESTORE DATABASE FROM THE LAST BACKUP
 - D. REPLACE COMPROMISED FILES WITH CLEAN VERSIONS
 - E. INSTALLING PATCHES; AND
 - F. ANY OTHER SYSTEM COMPONENTS.
- 36.11.2. THE CONTRACTOR SHALL ALSO WORK WITH SAM TO TEST IF THE RESTORED SYSTEM IS ABLE TO FUNCTION NORMALLY AT AN OPERATIONAL STATUS.
- 36.11.3. THE CONTRACTOR SHALL WORK OUT THE SCOPE, DURATION AND SCHEDULE FOR THE TEST, IN CONSULTATION WITH THE CUSTOMER AND ALL OTHER RELEVANT SERVICE PROVIDERS.
- 36.11.4. THE TEST SHALL ADDRESS AT LEAST THE FOLLOWING AREAS:
- A. RETRIEVAL OF THE BACKUP TAPES FROM OFF-SITE STORAGE;
 - B. SYSTEM RECOVERY FROM BACKUP MEDIA;
 - C. COORDINATION AMONG RECOVERY TEAMS
 - D. INTERNAL AND EXTERNAL CONNECTIVITY;
 - E. RESTORATION OF NORMAL OPERATIONS; AND
-

F. ACTIVATION PROCEDURES.

36.11.5. THE TEST SHALL BE CONDUCTED TO THE SATISFACTION OF SAM.

36.11.6. THE CONTRACTOR SHALL CONDUCT THE TEST IN A NON-PRODUCTION ENVIRONMENT AND ENSURE THAT THE TEST DO NOT CAUSE DISRUPTION TO THE NORMAL OPERATION OF THE SYSTEM.

37. OTHER GENERAL REQUIREMENTS**37.1. A Multi-Vendor Service Environment**

37.1.1. SEVERAL IT SUPPORT SERVICES IN SAM ARE CONTRACTED OUT TO OTHER THIRD-PARTY VENDORS. THIS INCLUDES, BUT NOT LIMITED TO:

- End-User helpdesk support;
- Server administration;
- Network infrastructure; and
- Other application development and maintenance.

37.1.2. THE AWARDED CONTRACTOR IS REQUIRED TO CO-OPERATE WITH THE OTHER THIRD-PARTY VENDORS TO ENSURE THAT THE SERVICE LEVELS FOR BOTH APPLICATIONS AND IT INFRASTRUCTURE ARE MET.

37.1.3. THE AWARDED CONTRACTOR, TOGETHER WITH SAM'S REPRESENTATIVE AND SAM'S THIRD PARTY VENDORS, SHALL MEET AS OFTEN AS REQUIRED BY SAM TO DISCUSS THE OPERATION ISSUES AND OTHER PROBLEMS THAT MAY BE ENCOUNTERED IN THE PROVISION OF THE SERVICES. THE RELEVANT PROJECT AND TECHNICAL MANAGERS OR OFFICERS INVOLVED IN THE PROVISION OF THE SERVICES SHALL ATTEND THE MEETINGS.

37.2. System Development and Testing Facilities

37.2.1. THE AWARDED CONTRACTOR SHALL ADHERE TO PART 2, SECTION A, CLAUSE 1.4(G) AND PART 2, SECTION B, CLAUSE 3 OF IDA(T)-1432(G) AND ANNEX C.

37.2.2. ALL SYSTEM MODULES SHALL BE BUILT MODULARLY FOR THE PURPOSE OF RE-USE.

37.2.3. NO HARD CODING WILL BE ACCEPTED, UNLESS OTHERWISE DISCUSSED WITH AND AGREED BY SAM. ALL PARAMETERS AND VARIABLES SHALL BE MADE CONFIGURABLE VIA THE SYSTEM WHERE POSSIBLE.

37.2.4. SYSTEM DESIGN, DEVELOPMENT AND TESTING SHALL BE CARRIED OUT AT THE AWARDED CONTRACTOR'S SITE. THE AWARDED CONTRACTOR SHALL HAVE ALL THE ESSENTIAL APPLICATION SOFTWARE AND LICENSES REQUIRED FOR THE DEVELOPMENT OF IGMS, INCLUDING TOOLS FOR MEASURING AND BENCHMARKING THE PERFORMANCE OF THE SYSTEMS.

37.2.5. THE AWARDED CONTRACTOR SHALL ENSURE THE DESIGN AND CHANGES OF IGMS SHALL NOT BE AFFECTED BY THE FOLLOWING LIST OF COMMON VULNERABILITIES, WHERE APPLICABLE, BUT NOT LIMITED TO THE FOLLOWING:

- a. Non-validated input (i.e. input fields shall conform to the desired formats and values);
- b. Broken access control;
- c. Broken authentication and session management (i.e. use of account credentials and session cookies);
- d. Cross-site scripting ("XSS");
- e. Buffer overflows;
- f. Injection vulnerability flaws (e.g. SQL injection, command injection etc.);
- g. Race conditions;
- h. Improper error / exception handling;
- i. Insecure storage;
- j. Denial of service; and
- k. Insecure configuration management.

37.2.6. THE AWARDED CONTRACTOR SHALL PROVIDE EVIDENCE THAT IGMS SHALL NOT BE AFFECTED BY THIS LIST OF COMMON VULNERABILITIES.

37.2.7. THE AWARDED CONTRACTOR SHALL MAKE SURE THAT ALL APPLICATION CODES ARE PROTECTED FROM WEB APPLICATION VULNERABILITIES (CROSS-SITE SCRIPTING, SQL INJECTION AND SO FORTH) AT ALL TIMES.

37.3. Confidentiality and Data Protection

37.3.1. EXCEPT WITH THE CONSENT IN WRITING BY THE SAM, CONTRACTORS SHALL NOT DISCLOSE THIS QUOTATION, OR ANY OF ITS PROVISIONS, SPECIFICATIONS, PLANS, DESIGNS, SAMPLES, OR INFORMATION ISSUED BY THE SAM.

37.3.2. CONTRACTORS SHALL TAKE ALL REASONABLE PRECAUTIONS IN DEALING WITH ANY INFORMATION DOCUMENTS AND PAPERS PASSED BY SAM TO THE CONTRACTOR SO AS TO PREVENT ANY UNAUTHORISED PERSON FROM HAVING ACCESS TO SUCH INFORMATION AND AGAINST LOSS.

37.3.3. CONTRACTORS AND ITS STAFF WHO ARE INVOLVED IN THIS PROJECT AND RFQ SHALL CONTINUE TO OBSERVE THE CONFIDENTIALITY AGREEMENT OF THE PROJECT EVEN AFTER THE PROJECT IS COMPLETED.

37.3.4. ALL STAFF ASSIGNED TO THE PROJECT SHALL OBSERVE THE CONFIDENTIALITY IN ACCORDANCE WITH THE OFFICIAL SECRETS ACT AND ANY OTHER INSTRUCTIONS AND DIRECTIVES.

37.3.5. THE CONTRACTOR SHALL OBSERVE THE REQUIREMENTS FOR SECURE USAGE AND HANDLING OF ALL GOVERNMENT INFORMATION. THE CONTRACTOR SHALL SUBJECT ALL THEIR PERSONNEL WHO WILL BE INVOLVED IN THE SYSTEM TO SECURITY CLEARANCE BY THE GOVERNMENT BEFORE COMMENCING THEIR WORK.

37.3.6. THE EMPLOYEES OF THE AWARDED CONTRACTOR SHALL, IF SO REQUIRED BY SAM, SIGN AN UNDERTAKING TO SAFEGUARD OFFICIAL INFORMATION.

37.4. Virus Free

37.4.1. ALL ITEMS PROVIDED BY THE AWARDED CONTRACTOR SHALL BE FREE OF COMPUTER VIRUS. FAILURE WHICH, THE AWARDED CONTRACTOR SHALL BE FULLY RESPONSIBLE AND SHALL MAKE GOOD ALL DATA LOSS, COST OF DOWNTIME, COST OF REMOVING THE COMPUTER VIRUS FROM ALL INFECTED ITEMS AND ANY OTHER COST INCURRED DUE TO THE COMPUTER VIRUS.

37.5. Copyrights

37.5.1. THE AWARDED CONTRACTOR SHALL MAKE SURE THAT ANY MATERIAL SUPPLIED BY THEM FOR THE DEVELOPMENT AND MAINTENANCE OF THE SYSTEMS DOES NOT VIOLATE OR INFRINGE ANY COPYRIGHT, TRADEMARK, PATENT, STATUTORY, COMMON LAW, OR PROPRIETARY LAW OF OTHERS.

37.6. Security Requirements

37.6.1. THE AWARDED CONTRACTOR SHALL COMPLY WITH SAM'S IT SECURITY STANDARDS, BEST PRACTICES AND CLAUSES LISTED UNDER ANNEX D.

37.6.2. THE AWARDED CONTRACTOR SHALL IDENTIFY ALL RISKS AND AS WELL AS ASSESS SECURITY THREATS ASSOCIATED WITH THE SYSTEM AND INCORPORATE THE PROPER CONTROLS TO MITIGATE THE RISKS IDENTIFIED, WHICH IS SUBJECT TO SAM'S APPROVAL.

37.6.3. THE GOVERNMENT RESERVES THE RIGHT TO HAVE SECURITY AUDIT, SECURITY REVIEW AND TESTING CONDUCTED ON THE SYSTEM AND ITS PREMISES BY THE GOVERNMENT AND / OR AN INDEPENDENT THIRD-PARTY ASSESSOR ENGAGED BY THE GOVERNMENT WHENEVER THE NEED ARISES. THE RIGHT TO AUDIT AND REVIEW SHALL ALSO BE EXTENDED TO THE AWARDED CONTRACTOR'S SUB-CONTRACTORS THAT ARE ALSO INVOLVED IN THE SYSTEM'S SERVICES, AS WELL AS OUTSOURCED SERVICES, SUPPORTING SYSTEMS AND PROCESSES THAT ARE MANAGED BY THE AWARDED CONTRACTOR AND SUB-CONTRACTORS. THE AWARDED CONTRACTOR SHALL WORK WITH THE GOVERNMENT AND / OR THE ASSESSOR TO PROVIDE THE NECESSARY SERVICES AND RESOURCES TO ASSIST IN THE SECURITY AUDIT, SECURITY REVIEW AND TESTING. THE SUPPLIER SHALL ALSO ENSURE THAT ANY RISKS AND / OR VULNERABILITIES IDENTIFIED ARE MITIGATED AND / OR RECTIFIED THROUGH PROPER CHANGE MANAGEMENT PROCESSES NO LATER THAN ONE (1) MONTH OR WITHIN A MUTUALLY AGREED PERIOD AFTER APPROVAL BY THE GOVERNMENT, AND AT NO ADDITIONAL COST TO THE GOVERNMENT.

37.7. Policies and Standards

37.7.1. THE AWARDED CONTRACTOR SHALL COMPLY TO THE LATEST VERSIONS OF THE POLICIES AND STANDARDS ISSUED BY THE GOVERNMENT, FOR EXAMPLE:

- a. PMO Cluster Security Policy;
- b. Instruction Manual (IM) Policy on ICT Security;
- c. IM Policy on Third Party Management; and
- d. Any other security policies, standards and guidelines that may be issued by the Government from time to time

37.7.2. A COPY OF THE ABOVE-MENTIONED DOCUMENTS CAN BE OBTAINED, AFTER THE AWARD OF THIS RFQ, FROM SAM AS REFERENCE FOR THE PURPOSE OF THIS PROJECT, WHERE APPLICABLE. THE AWARDED CONTRACTOR IS REQUIRED TO SIGN A NON-DISCLOSURE AGREEMENT FOR THE ABOVE. ALL COPIES SHALL BE RETURNED TO SAM AT THE EXPIRATION OR TERMINATION OF THIS CONTRACT,

37.7.3. WHEN REQUESTED BY SAM, THE AWARDED CONTRACTOR SHALL CONDUCT BRIEFING ON THE POLICIES AND STANDARDS INDICATED IN CLAUSE 12.7.1 TO ITS PERSONNEL AND SUB-CONTRACTORS.

37.8. Risk Management

37.8.1. THE CONTRACTORS SHALL PROPOSE A RISK MANAGEMENT PROCESS TO ASSESS SECURITY RISKS THAT IMPACT THE SYSTEM AND IMPLEMENT EFFECTIVE CONTROL MEASURES FOR MITIGATING THE RISKS. THE RISK MANAGEMENT PROCESS SHALL BE PROVIDED AS PART OF THE PROPOSAL SUBMISSION.

- 37.8.2. THE CONTRACTORS SHALL PROVIDE A DETAILED DESCRIPTION OF THEIR RISK MANAGEMENT PROCESS AND HOW IT WILL BE APPLIED TO THE SYSTEM. THE RISK MANAGEMENT PROCESS SHALL INCLUDE MINIMALLY THE FOLLOWING:
- a. Risk identification;
 - b. Risk assessment;
 - c. Risk response;
 - d. Risk control activities; and
 - e. Risk monitoring and review.
- 37.8.3. THE AWARDED CONTRACTOR SHALL DEVELOP, IMPLEMENT AND MAINTAIN THE RISK MANAGEMENT PROCESS FOR THE SYSTEM, AND THE GOVERNMENT SHALL RESERVE THE RIGHTS TO PROVIDE INPUT OR REQUEST AMENDMENTS TO THE RISK MANAGEMENT PROCESS AT NO ADDITIONAL COST TO THE GOVERNMENT. THE RISK MANAGEMENT PROCESS SHALL BE CONSISTENT WITH GOVERNMENT'S RISK MANAGEMENT METHODOLOGY AND IS SUBJECTED TO THE APPROVAL OF THE GOVERNMENT.
- 37.8.4. THE AWARDED CONTRACTOR SHALL IMPLEMENT APPROPRIATE CONTROL STRATEGIES THAT ARE CONSISTENT WITH THE GOVERNMENT SECURITY POLICIES AND STANDARDS, AND MITIGATE THE IDENTIFIED SECURITY RISKS.
- 37.8.5. THE AWARDED CONTRACTOR SHALL DEVELOP AND MAINTAIN THE RISK REGISTER SPECIFIC TO THE SYSTEM. THE RISK REGISTER SHALL DESCRIBE ALL OF THE IT SECURITY RISKS IDENTIFIED IN THE SYSTEM'S ENTIRE LIFECYCLE, AS WELL AS THE KEY RISK MANAGEMENT ACTIVITIES. THE RISK REGISTER, AS WELL AS ITS SUBSEQUENT UPDATES AND CHANGES, SHALL BE REVIEWED AND APPROVED BY THE GOVERNMENT.
- 37.8.6. THE AWARDED CONTRACTOR SHALL CONDUCT RISK ASSESSMENT AND REVIEW THE RISK REGISTER ON A REGULAR BASIS TO ENSURE THAT RISK MITIGATIONS REMAIN EFFECTIVE AS WELL AS TO IDENTIFY NEW INTERNAL AND EXTERNAL THREATS THAT MAY UNDERMINE THE SYSTEM SECURITY, INTERFERE WITH THE SYSTEM OR RESULT IN THE DESTRUCTION OF INFORMATION. THE FREQUENCY OF THE CONDUCT OF THE RISK ASSESSMENT AND ITS REVIEW SHALL BE MUTUALLY DETERMINED BETWEEN THE GOVERNMENT AND THE AWARDED CONTRACTOR. THE AWARDED CONTRACTOR SHALL SUBMIT THE SECURITY RISK ASSESSMENT REPORT TO THE GOVERNMENT WITHIN TWO (2) WEEKS UPON COMPLETION OF THE REVIEW.

37.9. Others

37.9.1. THE AWARDED CONTRACTOR SHALL BE RESPONSIBLE TO CO-ORDINATE AND WORK WITH THE TEAM(S) AUTHORISED BY THE GOVERNMENT TO ENSURE THE FINDINGS AND RECOMMENDATIONS FROM IT SECURITY AUDITS, WHICH MAY BE CARRIED OUT BY THE 3RD PARTY CONTRACTORS AUTHORISED BY THE GOVERNMENT FROM TIME TO TIME, ARE IMPLEMENTED FOR IGMS. THE AWARDED CONTRACTOR SHALL IMPLEMENT THE RECOMMENDATIONS:

- a. not later than one (1) week for critical findings from date of notification; and
- b. not later than four (4) weeks for non-critical findings from date of notification.

AFTER THE GOVERNMENT'S NOTIFICATION OF THE AUDIT FINDINGS AND RECOMMENDATIONS TO THE AWARDED CONTRACTOR.

37.9.2. THE AWARDED CONTRACTOR SHALL ADOPT THE QUALITY MANAGEMENT SYSTEM RECOMMENDED BY SAM.

38. DOCUMENTATIONS

38.1. The Awarded Contractor is responsible for the development and delivery of the following documentations for any major enhancements, upon mutual agreement:

- a. Impact Analysis, implementation plan and schedule;
- b. Requirements Specifications;
- c. System Design Specifications (if applicable);
- d. System Test Plan (including test cases) and Report (if applicable);
- e. Program Source Codes;
- f. UAT Test Plan (including test cases) and Report (if applicable);
- g. System Security Test Plan (if applicable);
- h. User Manual on the functionality and usage (if applicable);
- i. Monthly Progress Report; and
- j. Training Materials (if applicable).

38.2. The proposed Systems must not contain any hidden functionality and any knowledge that the SAM is not aware of. Such information, if any, shall be properly documented in one of the above documents.

38.3. All the documentations provided shall be of the latest version and shall also be written in English and expressed in a clear and easy to understand manner.

39. PAYMENT SCHEDULE AND BILLING

- 39.1. The payment for IGMS will be made on a monthly basis upon completion of maintenance and support services.
- 39.2. For CR, the Awarded Contractor shall bill SAM for the quoted effort upon successful completion and deployment of the CR in the production environment, and acceptance of the deliverables. SAM shall acknowledge and verify the quoted effort.
- 39.3. For any additional services/works orders for IGMS during the contract, the Awarded Contractor shall provide an invoice to SAM upon completion of the billed services/work orders. Only electronic invoices (e-invoices) are accepted.

40. VALIDITY OF RFQ

- 40.1. The proposal for this RFQ shall remain valid for a period of 6 months.

41. GUIDELINES FOR SUBMISSION

41.1. OVERALL GUIDELINES

- 41.1.1. THE CONTRACTORS SHALL SUBMIT THEIR PROPOSAL BASED ON THE SECTIONS LISTED BELOW. ANY NON-COMPLIANCE TO THIS FORMAT SHALL INVALIDATE THE PROPOSAL.

SECTION 1:PRICE SCHEDULE (REFER TO ANNEX I)

SECTION 2:STATEMENT OF COMPLIANCE (REFER TO ANNEX II)

SECTION 3:CONTRACTOR INFORMATION (REFER TO ANNEX III, IV AND V)

SECTION 4:PROPOSAL FOR SERVICES (REFER TO CLAUSE 16.5)

SECTION 5: OTHER INFORMATION

41.2. SECTION 1: PRICE SCHEDULE

- 41.2.1. THE CONTRACTOR MUST SUBMIT PRICES CLEARLY STATING THE FEES AND CHARGES, AND COST BREAKDOWN AS STATED IN ANNEX I. THE CUSTOMER SHALL NOT BE LIABLE FOR ANY PRICES NOT QUOTED BY THE CONTRACTOR IN THE PROPOSAL.

- 41.2.2. THE PRICES SHALL BE QUOTED IN HONG KONG DOLLARS AND EXCLUDE GST IN ALL COMPONENTS.
-

41.2.3. THE PRICES QUOTED SHALL BE EQUAL OR LOWER THAN THE PRICES AND RATES SET OUT IN THE MASTER CONTRACT JKT(R)5555-I.

41.2.4. THE PRICES QUOTED SHALL BE ALL INCLUSIVE (E.G. ANY REQUIRED OUT OF POCKET EXPENSES, FREIGHT AND DELIVERY CHARGES, INSURANCE, INSTALLATION AND ALL MATERIALS, MANUALS AND DOCUMENTATION REQUIRED OR IMPLIED) AND THE PRICING SHOULD BE GIVEN AT THE ITEMIZE LEVEL. NO FURTHER FEES OR CHARGES SHALL BE INCURRED OR PAYABLE BY THE CUSTOMER IN RESPECT OF THE ANY GOODS OR SERVICES PURCHASED UNDER THE CONTRACT.

41.3. **SECTION 2: STATEMENT OF COMPLIANCE**

41.3.1. THE CONTRACTOR SHALL INCLUDE IN A CLAUSE-BY-CLAUSE STATEMENT OF COMPLIANCE ACCORDING TO THE SECTION AND REFERENCES OF THIS RFQ AND STATE WHETHER THE SPECIFIED REQUIREMENTS CAN BE COMPLIED WITH, IN THE FORMAT AS SPECIFIED IN ANNEX II.

41.3.2. THE CONTRACTOR SHALL ENSURE THAT THE STATEMENT OF COMPLIANCE MUST ALSO INCLUDE ALL CLAUSES UNDER ANNEX C.

41.4. **SECTION 3: CONTRACTOR INFORMATION**

41.4.1. THE CONTRACTOR SHALL PROVIDE A BRIEF DESCRIPTION OF THE CONTRACTOR INFORMATION (ANNEX III), CONTRACTOR'S PERSONNEL INFORMATION (ANNEX IV) WHO WILL BE PERFORMING THE ABOVE IT APPLICATION MAINTENANCE AND SUPPORT, INCLUDING THE NUMBER OF YEARS OF IT APPLICATION MAINTENANCE AND SUPPORT EXPERIENCES, EDUCATION/PROFESSIONAL AND QUALIFICATIONS, AND CUSTOMER REFERENCES (ANNEX V) IN THE FORMAT SPECIFIED IN THE RESPECTIVE ANNEXES. CONTRACTOR SHALL SUBMIT 3 OR MORE CUSTOMER REFERENCES, EACH FROM A DIFFERENT GOVERNMENT AGENCY OR COMPANY.

41.5. **SECTION 4: PROPOSAL FOR SERVICES**

41.5.1. THIS SECTION SHALL CONTAIN A COMPREHENSIVE DESCRIPTION OF THE SERVICES PROPOSED BY THE CONTRACTOR. THE CONTRACTOR SHALL ENSURE THAT THE PROPOSED SERVICES MEET THE REQUIREMENTS STATED IN THIS RFQ.

41.5.2. IN ADDITION, THE CONTRACTOR SHALL INDICATE IN THEIR PROPOSAL ADDITIONAL INFORMATION RELATING TO CLAUSE 5.9.4, CLAUSE 5.9.6 AND CLAUSE 8.1.

42. EVALUATION APPROACH

- 42.1. The Contractors shall meet all critical criteria stated in Clause 17.3(A) before being shortlisted for further evaluation.
- 42.2. The evaluation approach shall be based on Price and Quality of the proposal. Price and Quality Attributes are assigned weightage and translated into quantitative scores which are then summed up to give a Combined score during the proposal evaluation.
- 42.3. The following criteria will be applied on all proposals during assessment:

(A) CRITICAL CRITERIA

- A. **CONTRACTORS MUST NOT BE DEBARRED ON OR AFTER THE CLOSING DATE OF THIS RFQ;**
- B. **COMPLETE SUBMISSION IN ACCORDANCE TO THE GENERAL LAYOUT STATED IN CLAUSE 16.1.**
- C. **FULL COMPLIANCE WITH ALL TERMS AND CONDITIONS DETAILED IN THE MASTER CONTRACT JKT(R)5555-I FOR APPLICATION DEVELOPMENT AND MAINTENANCE (ADM) AND THIS RFQ. A PROPOSAL THAT ATTEMPTS TO VARY THEM WILL BE REJECTED.**
- D. **CONTRACTORS SHALL NOTE THAT NON-COMPLIANCE WITH ANY OF THE ABOVE-MENTIONED CRITICAL CRITERIA SHALL EXCLUDE THE PROPOSAL FROM FURTHER EVALUATION.**

(B) EVALUATION CRITERIA

- (I) **PRICE COMPETITIVENESS; AND**
- (II) **QUALITY OF PROPOSAL AND EXPERIENCE OF THE PROPOSED TEAM, WHICH INCLUDES PROVEN CREDENTIALS AND TRACK RECORD OF PAST SIMILAR IT APPLICATION MAINTENANCE AND SUPPORT UNDERTAKEN BY THE CONTRACTOR.**

- 42.4. **THE PRICE SCORE (P-SCORE) WILL BE CALCULATED BASED ON THE FOLLOWING FORMULA:**
-

$$\text{P-Score} = \frac{\text{Lowest acceptable quotation price}}{\text{Contractor's price}} \times \text{Price Weightage (50\%)}$$

42.5. **THE PROPOSALS SHALL BE EVALUATED ACCORDING TO THE FOLLOWING QUALITY CRITERIA:**

S/N	Quality Criteria	Points awarded
1	Quality of proposal	20
2	Capabilities and Experience of Project Manager	30
3	Strength, Experience and Composition of Project Team (excluding Project Manager)	25
4	Contractor's Track Record in providing similar services in Hong Kong, including Customer Satisfaction	25
	Total points:	100

42.6. **THE QUALITY SCORE (Q-SCORE) WILL BE COMPUTED USING THE FOLLOWING FORMULA:**

$$\text{Q-Score} = \frac{\text{Contractor's total quality points}}{100} \times \text{Quality Weightage (50\%)}$$

42.7. **THE COMBINED SCORE OF AN RFQ PROPOSAL WILL BE THE SUM OF ITS PRICE SCORE AND QUALITY SCORE:**

$$\text{COMBINED SCORE} = \text{P-SCORE} + \text{Q-SCORE}$$

43. **ENQUIRIES**

- 43.1. Should Contractor have any enquiries on any aspect of this RFQ, the Contractor shall email the officers listed below:

Sample Text (Mr)
Email: Sample_text@gmail.com

Sample Text (Mr)

Email: Sample_text@gmail.com

Sample Text (Mr)

Email: Sample_text@gmail.com

ANNEX A – DETAILED INFORMATION OF IGMS

IGMS at a glance

Modules in IGMS

Module	Brief Description
Administration	Setup Host Institute Creation of accounts in Research Portal and AX Creation of accounts for reviewers Role Management
Dashboard	Research Portal dashboards for: Principal Investigator (PI) Reviewer Office of Research (ORE) / Academic Institution (AI) ORE Host Institution (HI) Finance HI Human Resources Director of Research (DOR)/ Alternate DOR/ AI DOR Dynamics AX 2012 dashboards for: Project Manager (PM) Agency Finance

	Research Grant Officer (RGO)
Grant Setup	Grant Programme Create and Modify Grant Call Create and Modify Open, Withdraw, Close
Grant Management	Proposal Submission New Proposal Submission ORE Verification DOR Endorsement PM Review PM seeks clarification from PI AI Verification and AID Endorsement Proposal Evaluation Peer Review Panel Review Panel Meeting Rebuttal Process Administer Outcome Pre award Budget/KPI and Milestone scrubbing HI ORE Verification PM Review PI Acceptance DOR Endorsement PM Acceptance Award Award Process ORE Verification DOR Endorsement AI Verification and AID Endorsement PM review process PM seeks Clarification from PI Proposal Closure

Deviation Management	New Deviation Submission ORE Verification DOR Endorsement PM Review
Finance Tracking	Honorarium Requests & Payments Fund Requisition & Payments (including Final Statement of Account) Cash Flow Projections Claims Reversal
Project Tracking	Project Creation Project Activation Project Monitoring and Control Progress Report Submission Progress Report Evaluation Progress Report Closure Equipment Tracking Project Closure
Reports	Pre-Award Reports Proposal Submission, Review of Proposal, Honorarium Request, until award Post-Award Reports KPI Tracking, Equipment Tracking, Deviation (non-virement), and Progress Report Submission Financial Reports Budget Tracking, Expense Request, Deviation (Virement) and Payment Other Reports User Account Information, Researcher Profiles, and Nationality Report

Roles in IGMS

Funding Agency Roles	Brief Description
Programme Manager (PM)	Launches the grant programme and grant calls Administers and manages the entire grant call
Agency Finance (AF)	Reviews and approves the Fund Requisitions in IGMS for the Grant Programme

Research Grant Officer (RGO)	Agency nominated representatives to ensure harmonisation of grant processes
Applicant/Host Institution Roles	Brief Description
Principal Investigator (PI)	Applies for the research grant Responsible for the management of the research project
Host Institution (HI)	The company the PI is employed in
Office of Research (ORE)	Typically the Director of Research's office Co-ordinates the grant management processes on behalf of the Host Institutions
Director of Research (DOR)	DOR endorses the proposal applications, the Letter of Award, deviations, progress reports, etc.
Host Institution Finance (HI Finance)	Submits the Fund Requisitions for the awarded research projects
Host Institution Human Resources (HI HR)	Updates the manpower list that is part of the Fund Requisitions
Reviewer	Assist with the evaluation of proposals Can be Primary, Secondary, Local, International or Expert Panellist (EP)

IGMS Pre-Award Process

a) Proposal Submission

b) Proposal Evaluation

c) Scrubbing

d) Award

IGMS Post-Award Process

a) Deviations / Progress Report

b) Fund Requisitions

ANNEX B – GCC CUSTOMER HANDBOOK

ANNEX C – CLAUSES IN EFFECT UPON EXPIRY OF IDA(T)-1432(G)

Description	Attachment
IDA(T)-1432(G): Part 1 Section B	

IDA(T)-1432(G): Part 1 Section B, Annex I	
IDA(T)-1432(G): Part 1 Section B, Annex II	

ANNEX D – OTHER SECURITY REQUIREMENTS**1.1. General**

- 1.1.1. THE CONTRACTOR SHALL FULLY COMPLY WITH ANY WRITTEN INSTRUCTIONS ON ICT SECURITY RELATED MATTERS THAT ARE ISSUED BY THE GOVERNMENT AND AUTHORITY FROM TIME TO TIME.
- 1.1.2. THE CONTRACTOR SHALL PLAN, IMPLEMENT AND MANAGE A SECURITY MANAGEMENT AND GOVERNANCE FRAMEWORK THAT COVERS SECURITY PROCEDURES AND STANDARDS. THE FRAMEWORK SHALL INCLUDE AT LEAST THE FOLLOWINGS:
- (a) Security Risk Management;
 - (b) Security Architecture and Design;
 - (c) Personnel Security;
 - (d) Security Incident and Response Management;
 - (e) Security Management and Operation Processes;
 - (f) Security Configuration;
 - (g) Security Reviews; and
 - (h) Audits for the System.
- 1.1.3. 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.
- 1.1.4. THE CONTRACTOR SHALL ENSURE THE SYSTEM AND PERSONNEL COMPLY WITH THE REQUIRED LEGISLATION, REGULATION AND CONTRACTUAL REQUIREMENTS.
- 1.1.5. THE CONTRACTOR SHALL ENSURE DATA AND INFORMATION IS PROTECTED FROM LEAKAGE, LOSS, DESTRUCTION AND FALSIFICATION IN ACCORDANCE WITH STATUTORY, REGULATORY, CONTRACTUAL AND BUSINESS REQUIREMENTS.
-

- 1.1.6. THE CONTRACTOR SHALL, AT NO ADDITIONAL COST TO SAM, CONDUCT YEARLY SELF-ASSESSMENT TO ENSURE IT CARRIES OUT THE ASSIGNED WORK UNDER THIS CONTRACT IN A MANNER THAT IS IN COMPLIANCE WITH THE CONTRACTUAL OBLIGATIONS AND APPLICABLE GOVERNMENT POLICIES AND STANDARDS. THE CONDUCT OF THE SELF-ASSESSMENT SHALL BE COMPLETED WITHIN A 2 MONTHS PERIOD. THE CONTRACTOR SHALL SUBMIT THE SELF-ASSESSMENT REPORT TO SAM WITHIN 1 MONTH OF THE COMPLETION OF THE SELF-ASSESSMENT.
- 1.1.7. THE CONTRACTOR SHALL, AT NO ADDITIONAL COST TO SAM, ENGAGE AN INDEPENDENT AUDITOR TO CONDUCT COMPLIANCE REVIEW ON THE CONTRACTOR THAT IT CARRIES OUT THE ASSIGNED WORK UNDER THIS CONTRACT IN A MANNER THAT IS IN COMPLIANCE WITH THE CONTRACTUAL OBLIGATIONS AND APPLICABLE GOVERNMENT POLICIES AND STANDARDS. THIS COMPLIANCE REVIEW SHALL BE CONDUCTED ONCE EVERY 3 YEARS. THE CONTRACTOR SHALL SUBMIT THE AUDIT REPORT WITHIN 1 MONTH OF THE COMPLETION OF THE AUDIT AND SUBMIT A REMEDIATION PLAN WITHIN 2 WEEKS OF THE DATE OF THE AUDIT REPORT TO SAM. THE REMEDIATION PLAN SHALL MINIMALLY INCLUDE THE TARGET REMEDIATION TIMELINES FOR ALL FINDINGS, WHICH SHALL BE NO LONGER THAN 12 MONTHS FROM DATE OF THE AUDIT REPORT. THE GOVERNMENT RESERVES THE RIGHT TO ENGAGE THE INDEPENDENT AUDITOR WHENEVER THE NEED ARISES, THE COST OF SUCH ENGAGEMENT SHALL BE FULLY BORNE BY THE CONTRACTOR.
- 1.1.8. THE CONTRACTOR SHALL, AT NO ADDITIONAL COST TO SAM, ENGAGE AN INDEPENDENT AUDITOR TO CONDUCT EXIT CHECKS TO ENSURE THE CONTRACTOR DISCONTINUES ITS SERVICES ACCORDING TO THE EXIT PLAN. THE CONTRACTOR SHALL SUBMIT THE AUDIT REPORT TO SAM WITHIN 1 MONTH OF THE COMPLETION OF THE AUDIT.

1.2. Security Risk Management

- 1.2.1. THE CONTRACTOR SHALL IMPLEMENT THE SECURITY RISK MANAGEMENT PROCESSES, STANDARDS AND PROCEDURES FOR THE SYSTEM WHICH SHALL ALIGN WITH THE AUTHORITY'S OVERALL RISK MANAGEMENT FRAMEWORK.
- 1.2.2. THE CONTRACTOR SHALL CONDUCT YEARLY ICT SECURITY RISK ASSESSMENTS TO IDENTIFY AND MANAGE INTERNAL AND EXTERNAL THREATS THAT MAY UNDERMINE THE SYSTEM SECURITY, INTERFERE WITH THE SYSTEM'S SERVICES OR RESULT IN THE UNAUTHORIZED DISCLOSURE OR DESTRUCTION OF INFORMATION. THE CONTRACTOR SHALL SUBMIT THE ICT SECURITY RISK ASSESSMENT REPORT TO THE AUTHORITY WITHIN 10 WORKING DAYS UPON THE COMPLETION OF EACH SECURITY RISK ASSESSMENT.
- 1.2.3. THE CONTRACTOR SHALL DESIGNATE AN IT SECURITY MANAGER (ITSM) TO PERFORM THE SCOPE OF WORK AS FOLLOWS:
- (a) Conduct IT Security Risk Assessment to identify the security threats to the System, assess the risk and determine controls to mitigate the risk, and
-

- (b) Provision of Risk Assessment Report, to act as an input to the Security Design Plan of the System that shall be produced by the Contractor.

1.2.4. THE CONTRACTOR SHALL DESIGNATE AN IT SECURITY MANAGER (ITSM) TO PERFORM THE SCOPE OF WORK AS FOLLOWS:

1.2.5. THE ITSM SHALL POSSESS THE NECESSARY SKILLS, KNOWLEDGE AND EXPERIENCE IN THE FOLLOWING AREAS:

- a) Security management frameworks and governance
- b) Security risk analysis and management
- c) Security incident response and management
- d) Technical expertise in proposed System platforms and technologies

1.2.6. THE ITSM SHALL BE BASED LOCALLY.

1.2.7. THE ITSM SHALL BE CONTACTABLE VIA MOBILE PHONE ON A 24X7 BASIS.

1.3. Vendor Certification & Competency

1.3.1. THE TENDERER SHALL STATE ANY SECURITY-RELATED CERTIFICATIONS THEY HAVE ATTAINED, SUCH AS ISO/IEC 27001 OR INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) V3, FOR THEIR SECURITY MANAGEMENT, GOVERNANCE FRAMEWORK AND OPERATIONS.

1.3.2. THE ITSM SHALL POSSESS RELEVANT SECURITY COMPETENCIES REQUIRED FOR THIS CONTRACT. AT A MINIMUM, THE INDEPENDENT IT SECURITY MANAGER SHALL POSSESS THE FOLLOWING:

- (a) A minimum of 3-year work experience in IT Security field
- (b) A valid Industry-accepted IT Security Professional Certifications (such as CISSP, CISA)
- (c) Comprehensive knowledge of International Standards and Best Practices for IT such as ISO/IEC 27001 and NSA Security Guidelines
- (d) Experienced in conducting Risk Assessments, Vulnerability Assessments, Security Audit, Penetration Testing and other IT Security tests.

Upon request by SAM, the Contractor shall produce such certifications obtained by the ITSM or customer reference describing such experience gained by the ITSM.

1.4. Security Incident and Response Management

- 1.4.1. THE CONTRACTOR SHALL PROPOSE, IMPLEMENT AND MAINTAIN A SECURITY INCIDENT HANDLING AND RESPONSE PLAN FOR THE SYSTEM. THE PLAN SHALL COMPLY AND BE CLOSELY INTEGRATED WITH THE AUTHORITY'S FRAMEWORK AND PROCEDURE FOR INCIDENTS MANAGEMENT.
- 1.4.2. THE CONTRACTOR SHALL ENSURE THAT ALL THEIR PERSONNEL ARE BRIEFED ON THE INCIDENT REPORTING PROCEDURES.
- 1.4.3. ALL SECURITY INCIDENTS SUCH AS VIRUS INFECTION, SECURITY COMPROMISES, UNAUTHORISED ACCESS AND SECURITY VULNERABILITY, SHALL BE REPORTED TO AUTHORITY IMMEDIATELY. THE CONTRACTOR SHALL TAKE THE NECESSARY ACTIONS TO ENSURE THAT ALL SECURITY INCIDENTS ARE PROPERLY HANDLED AND MANAGED.
- 1.4.4. IN THE EVENT OF ANY COMPUTER SECURITY INCIDENTS, THE CONTRACTOR'S RESPONSIBILITIES SHALL INCLUDE:
- a) Investigating, resolving and recovering from security incidents;
 - 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 security incident handling and response plan of the System.
- 1.4.5. THE CONTRACTOR SHALL GENERATE DETAIL INCIDENT INVESTIGATION REPORT FOR EACH INCIDENT AND SUBMIT IT TO THE AUTHORITY.
- 1.4.6. THE CONTRACTOR SHALL ALSO IMPLEMENT PREVENTIVE MEASURES TO THWART THE RECURRENCE OF SECURITY INCIDENTS.
- 1.4.7. THE CONTRACTOR SHALL GIVE FULL SUPPORT TO THE AUTHORITY IN RESOLVING THE SECURITY INCIDENTS BY ACTIVATING APPROPRIATE PERSONNEL AND RESOURCES FOR INVESTIGATION AND RESOLUTION PURPOSES.
- 1.4.8. THE SERVICE LEVEL FOR THE RESPONSE TIME, RESOLUTION TIME AND FREQUENCY OF STATUS UPDATE OF SECURITY INCIDENTS SHALL BE THE SAME AS THE SERVICE LEVEL STATED IN MASTER TENDER PART 2 SECTION 12, CLAUSE 12.1.3.
- 1.4.9. THE CONTRACTOR SHALL NOTE THAT SEVERITY LEVEL OF A SECURITY INCIDENT MAY BE ESCALATED OR REDUCED OVER TIME. FOR EXAMPLE, AN INCIDENT THAT IS CLASSIFIED AS SEVERITY LEVEL 2 MAY BE ESCALATED TO SEVERITY LEVEL 1 IF THE SERIOUSNESS OR IMPACT IS BIGGER THAN INITIALLY DETERMINED.
- 1.4.10. THE CONTRACTOR SHALL BE REQUIRED TO PERFORM ROOT CAUSE ANALYSIS ON ALL INCIDENTS. THE AUTHORITY, HOWEVER, RESERVES THE RIGHT TO UNDERTAKE PARALLEL INVESTIGATIONS OR TAKE OVER ANY ONGOING INVESTIGATIONS THAT IT DEEMS AS CRITICAL.
- 1.4.11. THE CONTRACTOR SHALL ENSURE THAT TOOLS USED IN THE ROOT CAUSE ANALYSIS ARE ABLE TO PRESERVE EVIDENCE FOR ADMISSION IN COURT.
-

- 1.4.12. THE CONTRACTOR SHALL ALSO COMPILE A MONTHLY REPORT SUMMARISING ALL SECURITY INCIDENTS THAT OCCUR WITHIN THE MONTH AND SUBMIT IT TO THE AUTHORITY.

1.5. Security Training and Awareness

- 1.5.1. THE CONTRACTOR SHALL ENSURE THAT ALL PERSONNEL ARE EQUIPPED WITH THE RELEVANT KNOWLEDGE, SKILLSETS AND EXPERIENCE TO IMPLEMENT AND MAINTAIN THE SYSTEM. THE PERSONNEL SHALL BE FAMILIAR WITH THE SECURITY REQUIREMENTS OF THE SYSTEM.
- 1.5.2. THE CONTRACTOR SHALL ENSURE THAT ALL THEIR PERSONNEL ARE INFORMED OF THEIR SECURITY RESPONSIBILITIES AND ACCOUNTABILITIES/LIABILITIES BEFORE PUTTING THE PERSON IN HIS/HER ASSIGNED AREAS OF WORK.
- 1.5.3. THE CONTRACTOR IS RESPONSIBLE TO IDENTIFY THEIR PERSONNEL'S SECURITY EDUCATION AND TRAINING NEEDS AND FORMULATE A LEARNING ROADMAP TO MEET THE NEEDS, ESPECIALLY FOR NEW RECRUITS AND THOSE TAKING ON NEW POSTS AND DUTIES FOR THIS CONTRACT.

1.6. Business Continuity Management

- 1.6.1. THE CONTRACTOR SHALL WORK WITH THE AUTHORITY TO DEVELOP AND DOCUMENT BUSINESS CONTINUITY FRAMEWORK AND PLAN TO ENSURE CORE BUSINESS OPERATIONS CAN CONTINUE WHEN DISRUPTIVE EVENTS OCCUR. WHEN REQUESTED BY SAM, THE CONTRACTOR SHALL ALSO PARTICIPATE IN SAM'S EXERCISE ON INCIDENT MANAGEMENT, BUSINESS CONTINUITY OR DISASTER RECOVERY WITH REGARDS TO THE IGMS. THE PLAN SHALL MINIMALLY INCLUDE:
- (a) Security considerations,
 - (b) Emergency response,
 - (c) Incident response,
 - (d) Recovery procedure, and

1.7. Security Access Control

- 1.7.1. THE CONTRACTOR SHALL ENSURE THAT ACCESS RIGHTS ARE GRANTED BASED ON JOB NEEDS.
- 1.7.2. THE CONTRACTOR SHALL REVIEW THE ACCESS RIGHTS ON REGULAR BASIS. THE CONTRACTOR SHALL IMPLEMENT MEASURES TO ENSURE THAT REDUNDANT USER ACCOUNTS AND ACCESS RIGHTS ARE SUSPENDED WHEN THEY ARE NOT USED FOR NINETY (90) 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.
-

- 1.7.3. THE CONTRACTOR SHALL ENSURE THAT ALL ACCOUNTS (I.E. ADMINISTRATIVE, FUNCTIONAL 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.
- 1.7.4. 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).
- 1.7.5. THE CONTRACTOR SHALL PROVIDE IMPLEMENT SECURITY CONTROL MEASURES AND PROCEDURES TO PREVENT UNAUTHORISED ACCESS TO SYSTEM MANAGEMENT CONSOLES.
- 1.7.6. THE CONTRACTOR SHALL HAVE PROPER APPROVAL PROCESS AND TRACKING MECHANISM FOR ALL ACCESS TO THE SYSTEM AND INFORMATION TO ENSURE PROPER USAGE AND ACCOUNTABILITY.
- 1.7.7. THE CONTRACTOR SHALL IMPLEMENT PHYSICAL SECURITY CONTROL MEASURES AND PROCEDURES TO PREVENT ANY UNAUTHORISED ACCESS TO THE SYSTEM.
- 1.7.8. THE CONTRACTOR SHALL NOT ALLOW REMOTE ACCESS TO THE SYSTEMS AND NETWORK UNLESS THE ACCESS IS PROPERLY JUSTIFIED AND APPROVED BY THE AUTHORITY. AGENCIES SHALL IMPLEMENT ALL OF 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 2-factor authentication to authenticate to the servers and applications; and
 - d) Logging of the date time, IP addresses of the source and destination systems, user information as well as the type of action performed shall be enabled on the servers that allow remote administrative access.

1.8. Data Confidentiality and Integrity

- 1.8.1. 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).
-

1.8.2. WHEN REQUESTED BY THE AUTHORITY, THE CONTRACTOR SHALL PROVIDE DETAILED DESCRIPTION OF THE CONTROL MEASURES.

1.8.3. THE CONTRACTOR SHALL IMPLEMENT ALL NECESSARY MEASURES AND PROCESSES TO PREVENT UNAUTHORISED DISCLOSURE, MODIFICATION OR DELETION OF AUTHORITY'S SECURITY-CLASSIFIED INFORMATION.

1.9. Personal Data

1.9.1. THE CONTRACTOR SHALL TAKE ALL REASONABLE MEASURES TO ENSURE THAT PERSONAL DATA HELD IN CONNECTION WITH THIS CONTRACT IS PROTECTED AGAINST LOSS, AND AGAINST UNAUTHORISED ACCESS, USE, MODIFICATION, DISCLOSURE OR OTHER MISUSE.

1.9.2. THE CONTRACTOR SHALL IN RESPECT OF ANY PERSONAL DATA HELD IN CONNECTION WITH THE CONTRACT COOPERATE WITH ANY REASONABLE REQUESTS, DIRECTIONS OR GUIDELINES OF THE AUTHORITY ARISING IN CONNECTION WITH THE HANDLING OF PERSONAL DATA.

1.10. Asset and Information Security

1.10.1. THE CONTRACTOR IS REQUIRED TO MAINTAIN STRICT CONFIDENTIALITY AND ENSURE THAT ALL INFORMATION PERTAINING TO ANY PREMISES THAT THE SERVICES ARE BEING CARRIED OUT FROM AND THE AUTHORITY'S WORK ENVIRONMENT MUST NOT BE DISCLOSED TO ANYONE EXCEPT THE REPRESENTATIVE AND THE CONTRACTOR'S EMPLOYEES, AGENTS OR SUB-CONTRACTORS DIRECTLY INVOLVED IN PERFORMING THE OBLIGATIONS UNDER THIS CONTRACT. THE CONTRACTOR IS TO ENSURE THAT INFORMATION IS NOT TO BE PUBLISHED OR COMMUNICATED TO ANY OTHER PERSON IN ANY FORM WHATSOEVER EXCEPT ON A STRICTLY "NEED-TO-KNOW" BASIS. FAILURE TO COMPLY WITH THIS CONFIDENTIALITY REQUIREMENT SHALL BE A GROUND FOR TERMINATION OF THIS CONTRACT.

1.10.2. 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 AUTHORITY. THE CONTRACTOR SHALL BE RESPONSIBLE FOR THE SAFEGUARDING OF SECURITY-CLASSIFIED INFORMATION UNDER THEIR CARE.

1.10.3. THE CONTRACTOR'S PERSONNEL SHALL SIGN CONFIDENTIALITY AGREEMENTS PRESCRIBED BY THE AUTHORITY TO ENSURE NO UNAUTHORIZED DISCLOSURES OF SECURITY-CLASSIFIED OR SENSITIVE INFORMATION RECEIVED OR GENERATED UNDER THIS TENDER OR CONTRACT UNLESS SPECIFICALLY AUTHORIZED BY THE AUTHORITY IN WRITING.

1.10.4. THE CONTRACTOR SHALL MAINTAIN AN INVENTORY OF ALL MATERIALS AND ASSETS RELEVANT TO THIS CONTRACT, AND UPDATE THE AUTHORITY BEFORE THE END OF NEXT MONTH UPON A CHANGE IN THE INVENTORY IN THE CURRENT MONTH. THE INVENTORY SHALL MINIMALLY CONSIST OF HARDWARE, SOFTWARE, PERSONNEL AND DOCUMENTATION SUCH AS PROJECT PLAN, INCIDENT/ PROGRESS REPORT, STANDARD OPERATION PROCEDURES AND SYSTEM CONFIGURATIONS.

- 1.10.5. 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 AUTHORITY. 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.
- 1.10.6. THE CONTRACTOR SHALL ENSURE THE AUTHORITY'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.
- 1.10.7. ANY LOSS OF THE AUTHORITY'S ASSETS AND/OR INFORMATION SHALL BE REPORTED IMMEDIATELY IN ACCORDANCE WITH THE AUTHORITY'S SECURITY INCIDENT RESPONSE PLAN.
- 1.10.8. 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 AUTHORITY. 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 AUTHORITY. 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 SHALL ENSURE THAT DISCUSSIONS ARE NOT CONDUCTED IN PUBLIC AREAS SUCH AS CAFES AND RESTAURANTS.
- 1.10.9. INFORMATION THAT HAS BEEN DECLASSIFIED IS NOT AUTOMATICALLY AUTHORISED FOR PUBLIC DISCLOSURE. THE CONTRACTOR SHALL REQUEST FOR APPROVAL FOR PUBLIC DISCLOSURE OF SUCH DECLASSIFIED INFORMATION FROM THE AUTHORITY.
- 1.10.10. THE CONTRACTOR SHALL ENSURE THAT ASSETS AND INFORMATION ARE NOT TAKEN OUT OF COUNTRY AND THE PREMISES USED TO PERFORM SERVICES UNDER THIS CONTRACT WITHOUT PRIOR APPROVAL IN WRITING BY THE AUTHORITY.
- 1.10.11. THE CONTRACTOR SHALL NOT TRANSFER SECURITY-CLASSIFIED INFORMATION OR PERSONAL DATA HELD IN CONNECTION WITH THIS CONTRACT OUTSIDE HONG KONG, OR ALLOW PARTIES OUTSIDE HONG KONG TO HAVE ACCESS TO IT, WITHOUT PRIOR APPROVAL IN WRITING BY THE AUTHORITY.
- 1.10.12. THE CONTRACTOR SHALL ENSURE THAT NO PERSON REMOVE ANY SECURITY-CLASSIFIED INFORMATION UPON RESIGNATION FROM HIS/HER APPOINTMENT OR RETAIN SUCH INFORMATION WHEN HE / SHE NO LONGER REQUIRES THEM.
-

- 1.10.13. 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.
- 1.10.14. THE CONTRACTOR SHALL IMMEDIATELY NOTIFY THE AUTHORITY WHEN IT BECOMES AWARE THAT A DISCLOSURE OF ANY SECURITY-CLASSIFIED OR SENSITIVE INFORMATION ACQUIRED IN CONNECTION WITH THIS CONTRACT.
- 1.10.15. TERMINATION/EXPIRATION OF THIS CONTRACT FOR WHATEVER CAUSE SHALL NOT PUT AN END TO THE OBLIGATION OF CONFIDENTIALITY IMPOSED ON THE CONTRACTOR, ITS EMPLOYEES, AGENTS AND/OR SUBCONTRACTORS UNDER THIS CLAUSE.

1.11. Security Architecture and Design

- 1.11.1. 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.
 - 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.
- 1.11.2. 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.
- 1.11.3. 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 AUTHORITY.
- 1.11.4. THE CONTRACTOR SHALL ENSURE THAT SEPARATE ENVIRONMENTS ARE IMPLEMENTED FOR SYSTEM DEVELOPMENT, TESTING, TRAINING, STAGING AND PRODUCTION.
- 1.11.5. THE CONTRACTOR SHALL CONDUCT CHECKS ON ITS FUNCTIONAL CAPABILITIES AND IMPLEMENTATION TO ENSURE THAT ADEQUATE SECURITY MEASURES ARE TAKEN THROUGHOUT THE ENTIRE LIFECYCLE OF THE SYSTEM.
-

- 1.11.6. 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 DOCUMENT AND PROPOSE MITIGATION MEASURES FOR THE AUTHORITY TO CONSIDER AND APPROVE BEFORE IMPLEMENTATION.
- 1.11.7. 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-LIFE (EOL).
- 1.11.8. 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.
- 1.11.9. THE CONTRACTOR SHALL IMPLEMENT ANTI-VIRUS OR ANTI-MALWARE SOFTWARE TO PREVENT, DETECT (ON-ACCESS AND ON-DEMAND) AND REMOVE MALICIOUS CODES FROM SYSTEMS OR DEVICES, AND ENSURE THAT THE DEFINITION 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 DEFINITION FILE SHALL BE UPDATED ON REGULAR BASIS.
- 1.11.10. THE CONTRACTOR SHALL ENSURE THE NECESSARY SECURITY CONTROLS ARE IMPLEMENTED TO HANDLE THE FOLLOWING:
- A) INPUT VALIDATIONS,
 - B) WORKFLOW CONTROLS,
 - C) MESSAGE INTEGRITY, AND
 - D) OUTPUT VALIDATIONS
- 1.11.11. 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, AND
- J) INSUFFICIENT LOGGING & MONITORING.

1.11.12. THE CONTRACTOR IS TO MAKE REFERENCE TO 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.

1.11.13. THE TENDERER SHALL DEVELOP AND MAINTAIN A SECURITY GUIDELINES DOCUMENT COVERING THE SCOPE OF THE SYSTEM BASED ON MINIMALLY:

- A) THE AUTHORITY'S SECURITY STANDARDS AND POLICIES,
- B) COMPLIANCE WITH REGULATIONS TO DATA PRIVACY,
- C) DATA HANDLING, AND
- D) SECURE CODING PROCEDURES IN THE LANGUAGE CHOSEN FOR THE APPLICATION.

1.11.14. THE CONTENT OF THE SECURITY GUIDELINES DOCUMENT SHALL BE DISCUSSED, REVIEWED AND APPROVED BY THE AUTHORITY.

1.11.15. NOTWITHSTANDING ACCEPTANCE BY THE AUTHORITY TO ANY OF THE TENDERER'S PROPOSAL, DESIGN AND SPECIFICATIONS, THE CONTRACTOR SHALL REMAIN SOLELY RESPONSIBLE FOR THE COMPLETENESS AND ADEQUACY OF THE DESIGN, PERFORMANCE AND SPECIFICATIONS OF THE WORKS.

1.12. Application and System Security

1.12.1. THE CONTRACTOR SHALL ENSURE THAT SECURITY IS A KEY CONSIDERATION AT EACH STAGE OF THE SOFTWARE DEVELOPMENT LIFECYCLE. THE CONTRACTOR SHALL IDENTIFY SECURITY WEAKNESSES, PROPOSE MITIGATION AND IMPROVEMENT MEASURES FOR REVIEW WITH THE AUTHORITY.

1.12.2. THE CONTRACTOR SHALL INCORPORATE SECURITY REQUIREMENTS INTO THE SOFTWARE DEVELOPMENT LIFECYCLE 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 AUTHORITY.

- 1.12.3. IN THE EVENT OF DEPLOYMENT OF ANY COMMERCIAL-OFF-THE-SHELF (COTS) SOFTWARE, THE CONTRACTOR SHALL PRODUCE A SECURITY RISK PROFILE FOR THE SOFTWARE. ANY SECURITY VULNERABILITY OR WEAKNESS SHALL BE DOCUMENTED AND HIGHLIGHTED TO THE AUTHORITY ABOUT ITS IMPLICATIONS. THE DECISION TO DEPLOY THE SOFTWARE WITH ANY WORKAROUND OR FIXES SHALL BE REVIEWED AND AGREED WITH THE AUTHORITY.
- 1.12.4. THE CONTRACTOR SHALL USE SECURITY CONTROL LIBRARIES SUCH AS OWASP'S ENTERPRISE SECURITY API (ESAPI) FOR THE PROGRAMMING LANGUAGES OF CHOICE, 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.
- 1.12.5. 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,
 - 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
 - f) Escaping of all un-trusted data in HTML contexts
- 1.12.6. THE CONTRACTOR SHALL IMPLEMENT APPROPRIATE APPLICATION EXCEPTION HANDLING MECHANISMS TO DISPLAY SIMPLIFIED 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.
- 1.12.7. THE CONTRACTOR SHALL IMPLEMENT APPROPRIATE SESSION MANAGEMENT FOR APPLICATION SUBJECTED TO APPROVAL BY THE AUTHORITY. THE IMPLEMENTATION SHALL MINIMALLY COVER:
- A) CONFIGURABLE SESSION TIMEOUT PERIODS (USUALLY 15 MINUTES BUT CAN BE CHANGED),
 - B) SECURE TRANSMISSION OF SESSION ID, AND
 - C) SESSION ID IN THE COOKIE INSTEAD OF URL.
-

1.12.8. THE CONTRACTOR SHALL IMPLEMENT APPROPRIATE SECURITY MEASURES TO ENSURE THAT TRANSPORT LEVEL SECURITY MEASURES (FOR EXAMPLE TLS, ETC.) ARE IMPLEMENTED SUBJECT TO APPROVAL BY THE AUTHORITY. THE MEASURES SHALL MINIMALLY CONSIDER THE FOLLOWING:

- (A) ENABLE AT LEAST TLS 1.2 FOR ALL SENSITIVE PAGES,
- (B) SET THE SECURE FLAG ON ALL SENSITIVE COOKIES,
- (C) SET THE HTTPONLY FLAG ON ALL SENSITIVE COOKIES
- (D) USE ONLY STRONG CIPHER SUITES,
- (E) USE VALID DIGITAL CERTIFICATES. EXTENDED VALIDATION (EV) DIGITAL CERTIFICATE MUST BE USED FOR INTERNET-ACCESSIBLE APPLICATION SYSTEMS THAT PERFORM ONLINE INTERACTIONS OR DATA CAPTURES, AND
- (F) SECURE BACKEND CONNECTIONS

1.12.9. 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.

1.12.10. THE CONTRACTOR SHALL IMPLEMENT APPROPRIATE MEASURES TO PROTECT CLASSIFIED AND SENSITIVE DATA IN-TRANSIT AND AT-REST. THESE MEASURES SHALL BE SUBJECT TO ACCEPTANCE BY THE AUTHORITY.

1.12.11. 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.

1.12.12. THE CONTRACTOR SHALL ENSURE THAT ALL PROPOSED CRYPTOGRAPHIC-BASED CONTROLS IMPLEMENTATION IN THE SYSTEM SUPPORTS MINIMALLY THE FOLLOWING ALGORITHMS OR ITS EQUIVALENT:

- (A) SYMMETRIC ENCRYPTION: AES WITH KEY SIZES OF AT LEAST 256 BITS,
 - (B) ASYMMETRIC ENCRYPTION: RSA PUBLIC KEY ENCRYPTION WITH KEY SIZES OF AT LEAST 2048 BITS,
-

- (C) DIGITAL SIGNATURE: DIGITAL SIGNATURE ALGORITHM (COMPLIANCE TO FIPS 186-3),
- (D) HASH ALGORITHM: SHA-2 OR SHA-3 OF AT LEAST 384 BITS,
- (E) KEY EXCHANGE: ELLIPTIC CURVE DIFFIE-HELLMAN (ECDH) (SUPPORTING P-256 AND B-283 CURVES).

- 1.12.13. THE SYSTEM 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.
- 1.12.14. THE CONTRACTOR SHALL ENSURE THAT ANY WEB-AUTHORING FUNCTIONALITY, E.G. VIA WEBDAV-BASED FEATURES, IS MADE AVAILABLE TO AUTHENTICATED, APPROVED USERS ONLY.
- 1.12.15. 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.
- 1.12.16. THE CONTRACTOR SHALL ENSURE THAT WHERE A WEB SOURCE OFFERS BOTH HTTP AND HTTPS ACCESS, THE SYSTEM WILL USE HTTPS FOR RETRIEVING AND TRANSPORTING DATA.
- 1.12.17. 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 AUTHORITY.
- 1.12.18. THE CONTRACTOR SHALL ENSURE THAT ALL ADMINISTRATION MODULES OF THE SYSTEM ARE ACCESSIBLE ONLY FROM PRE-IDENTIFIED NETWORK ADDRESSES.
- 1.12.19. THE CONTRACTOR SHALL ENSURE ALL CONFIDENTIAL AND RESTRICTED ACCESS SECTIONS OF THE SYSTEM ARE PROTECTED BY AUTHENTICATION AND PROPER ACCESS CONTROL.
- 1.12.20. THE CONTRACTOR SHALL ENSURE SECURITY PENETRATION TESTING IS CARRIED OUT ON THE SYSTEM PRIOR TO DEPLOYMENT. THE SECURITY PENETRATION TEST PLANS SHALL BE AGREED BY THE AUTHORITY BEFORE CONDUCTING THE TEST.
- 1.12.21. 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.
- 1.12.22. THE CONTRACTOR SHALL ENSURE ALL TEST DATA AND ACCOUNTS ARE REMOVED FROM PRODUCTION SYSTEM BEFORE SYSTEM COMMISSIONING.
-

1.13. Unauthorised Code

- 1.13.1. IN THIS CLAUSE, “UNAUTHORISED CODE” MEANS ANY VIRUS, TROJAN HORSE, WORM, LOGIC BOMB OR OTHER SOFTWARE ROUTINE OR HARDWARE COMPONENTS DESIGNED TO PERMIT UNAUTHORISED ACCESS, TO DISABLE, ERASE, OR OTHERWISE HARM SOFTWARE, HARDWARE OR DATA, OR TO PERFORM ANY SUCH ACTIONS.
- 1.13.2. THE CONTRACTOR WARRANTS THAT ALL MAGNETIC OR OTHER STORAGE MEDIA AND OTHER MATERIALS CAPABLE OF BEING STORED ON SUCH MEDIA, WHETHER SUPPLIED AS A SOFTWARE OR PART THEREOF OR WITH ANY SOFTWARE, OR USED IN THE PERFORMANCE OF ANY SERVICES SHALL NOT CONTAIN ANY UNAUTHORISED CODE.
- 1.13.3. PRIOR TO AND AT THE TIME OF SOFTWARE DELIVERY AND INSTALLATION, THE CONTRACTOR SHALL CONDUCT A COMPLETE AND THOROUGH SCAN FOR UNAUTHORISED CODE USING A RELIABLE ANTI-VIRUS SOFTWARE PACKAGES(S) ON ALL SOFTWARE AND MATERIALS PROVIDED UNDER THIS CONTRACT.
- 1.13.4. IN THE CASE OF BREACH OF CLAUSE 1.14.2 ABOVE, THE CONTRACTOR SHALL INDEMNIFY THE AUTHORITY FULLY AGAINST ALL COSTS INCURRED BY THE GOVERNMENT IN THE COURSE OF OR INCIDENTAL TO REMOVING THE UNAUTHORISED CODE AND RECOVERING ANY LOST OR DAMAGED DATA OR SOFTWARE. THE CONTRACTOR SHALL PAY THE AUTHORITY A SUM OF HONG KONG DOLLARS ONE THOUSAND SIX HUNDRED (\$\$1,600) OR 2 MAN-DAYS WORTH OF CHANGE REQUESTS FOR EACH SUCH DISCOVERY AS LIQUIDATED DAMAGES, BEING A GENUINE PRE-ESTIMATE OF THE ADMINISTRATIVE COST (INCLUDING COSTS ARISING FROM INVESTIGATIVE EFFORTS) OCCASIONED BY THE DISCOVERY OF AN UNAUTHORISED CODE.
- 1.13.5. IF, AFTER THE PERFORMANCE OF ANY MAINTENANCE SERVICES, THE SYSTEM IS DISCOVERED TO CONTAIN OR BE AFFECTED BY ANY UNAUTHORISED CODE AND IT IS SHOWN THAT THIS WAS THE RESULT OF ANY DEFAULT OF OR NEGLIGENT ACT OR OMISSION OF THE CONTRACTOR, ITS SUB-CONTRACTOR, OR THEIR RESPECTIVE EMPLOYEES, THE CONTRACTOR SHALL INDEMNIFY THE AUTHORITY FULLY AGAINST ALL COSTS INCURRED BY THEM IN THE COURSE OF OR INCIDENTAL TO REMOVING THE UNAUTHORISED CODE AND RECOVERING ANY LOST OR DAMAGED DATA OR SOFTWARE. THE CONTRACTOR SHALL PAY THE AUTHORITY A SUM OF HONG KONG DOLLARS ONE THOUSAND SIX HUNDRED (\$\$1,600) OR 2 MAN-DAYS WORTH OF CHANGE REQUESTS FOR EACH SUCH DISCOVERY AS LIQUIDATED DAMAGES, BEING A GENUINE PRE-ESTIMATE OF THE ADMINISTRATIVE COST (INCLUDING COSTS ARISING FROM INVESTIGATIVE EFFORTS) OCCASIONED BY THE DISCOVERY OF AN UNAUTHORISED CODE.

1.14. Authentication and Password Security

- 1.14.1. THE CONTRACTOR SHALL PUT IN PLACE STRONG AUTHENTICATION AND ACCESS CONTROL MECHANISMS TO ENSURE THAT ONLY AUTHORISED USERS ARE GRANTED ACCESS TO CONTROLLED FEATURES (E.G. PERSONALIZED VIEWS).
-

1.14.2. THE SYSTEM SHALL 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.

1.14.3. THE SYSTEM SHALL IMPLEMENT THE FOLLOWING FEATURES WHEN USING PASSWORDS:

- (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 change once every TWELVE (12) months;
 - (d) Prohibit password reuse for a minimum of THREE (3) generations;
 - (e) Passwords must not be displayed in clear;
 - (f) Transmit only cryptographically protected passwords (e.g. encryption of passwords at application layer before transmitting over a secure channel);
 - (g) 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 32-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
 - vi. function (e.g. PBKDF2). The cost factor should be at least 10,000 iterations.
 - (h) Passwords to be changed upon the first login; Passwords cannot be the same as account ID or user ID;
 - (i) Limit consecutive failed authentication attempts that can be made on a single account to TEN (10) times or less;
 - (j) System must be protected against dictionary or brute-force attacks; and
-

- (k) For internet-accessible application systems, the system must reject commonly used, expected or compromised passwords. To assist users, the reason for rejection must be provided.

1.14.4. THE CONTRACTOR SHALL ENSURE GENERIC AUTHENTICATION RESPONSES FOR LOGIN ERRORS.

1.14.5. THE CONTRACTOR SHALL ENSURE USE OF MULTI-FACTOR AUTHENTICATION FOR ADMINISTRATORS (E.G. SYSTEM ADMINISTRATOR, NETWORK ADMINISTRATOR, DATABASE ADMINISTRATOR), OPERATORS AND OTHER PRIVILEGED USERS.

1.14.6. THE CONTRACTOR SHALL ENSURE USE OF MULTI-FACTOR AUTHENTICATION FOR <END-USERS >.

1.15. Change Management

1.15.1. THE CONTRACTOR SHALL DEVELOP AND MAINTAIN DETAILED CONFIGURATIONS DOCUMENTATIONS OF THE SYSTEM FROM THE APPLICATIONS DOWN TO THE SERVER LEVEL.

1.15.2. THE CONTRACTOR SHALL IMPLEMENT A CHANGE CONTROL PROCESS TO ENSURE THAT ALL INTENDED CHANGES TO THE ORIGINAL CONFIGURATIONS AND/OR CHANGES TO THE PRODUCTION ENVIRONMENT ARE PROPERLY REVIEWED, TESTED AND AUTHORISED BEFORE IMPLEMENTATIONS.

1.16. Vulnerability and Patch Management

1.16.1. THE CONTRACTOR SHALL IMPLEMENT AND OPERATE THE NECESSARY INFRASTRUCTURE AND PROCESSES TO CONTROL THE DEPLOYMENT AND MAINTENANCE OF INTERIM SOFTWARE RELEASES INTO THE SYSTEM. THIS IS TO HELP MAINTAIN OPERATIONAL EFFICIENCY, EFFECTIVENESS AND STABILITY OF THE SYSTEM, AND TO OVERCOME KNOWN SECURITY VULNERABILITIES.

1.16.2. 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,
- (b) Identification of new software update,
- (c) Evaluation and planning of software update, and
- (d) Deployment of software update.

1.16.3. THE CONTRACTOR SHALL PROACTIVELY MONITOR INFORMATION ABOUT NEW SOFTWARE UPDATES ON A MONTHLY BASIS.

1.16.4. THE CONTRACTOR SHALL DETERMINE WHETHER THE SOFTWARE UPDATE SHOULD BE CONSIDERED A NORMAL CHANGE OR AN EMERGENCY ONE.

1.16.5. UPON EVALUATION, THE CONTRACTOR SHALL SUBMIT A REQUEST FOR CHANGE TO THE AUTHORITY TO SEEK APPROVAL TO DEPLOY THE SOFTWARE UPDATE. THE SUBMISSION OF THE REQUEST TO THE AUTHORITY 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 AUTHORITY.

1.16.6. THE CONTRACTOR SHALL ENSURE SECURITY AND RELEVANT PATCHES, WHEN RELEASED OFFICIALLY BY THE VENDORS OR WHEN NOTIFIED BY THE GOVERNMENT, 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
Internet-accessible Application Systems Service-Wide Systems and Infrastructures	High	ONE (1) month
	Medium / Low	TWO (2) months
Intranet Application Systems	High	TWO (2) months
	Medium / Low	THREE (3) months

TABLE 1: DEPLOYMENT TYPE AND SCHEDULE

1.16.7. THE CONTRACTOR SHALL SUBMIT THE TEST RESULTS TO THE AUTHORITY TO SEEK APPROVAL FOR DEPLOYMENT TO PROCEED. THE SUBMISSION SHALL INCLUDE A ROLLBACK PLAN. THE SUBMISSION SHALL ALSO INCLUDE ANY FORWARD SCHEDULE OF CHANGE AND USER COMMUNICATIONS MESSAGES.

1.16.8. THE CONTRACTOR SHALL ENSURE THAT VULNERABILITY ASSESSMENT USING INDUSTRY RECOGNISED TOOLS IS PERFORMED ON THE SYSTEM ON A QUARTERLY BASIS.

1.16.9. 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 AUTHORITY.

1.17. System Audit Logging

1.17.1. 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.

1.17.2. THE SYSTEM SHALL PROVIDE 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 (for e.g. add / delete / amend user accounts and profiles);
- b) System administration activities (for e.g. add / delete / amend system configuration);
- c) System backup and recovery activities;
- d) User log in and out activities;
- e) Successful and unsuccessful attempts to logins and logouts of the System;
- f) Use of privileged functions and utilities;
- g) Access violations from local and remote requests;
- h) Service start up and shutdown;
- i) Service backup and recovery; and
- j) Configuration changes.

1.17.3. THE SYSTEM SHALL BE CAPABLE OF LOGGING TRANSACTION PERFORMED BY USERS (E.G. ADDING, EDITING, AND DELETION OF RECORDS, CASES, DOCUMENTS). THE AUTHORITY RESERVES THE RIGHTS TO DECIDE ON THE TYPES OF USER ACTIVITIES TO BE LOGGED IN THE AUDIT TRAILS.

1.17.4. THE INFORMATION IN AUDIT LOGS SHALL 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.

1.17.5. THE CONTRACTOR SHALL IDENTIFY AND INCLUDE ADDITIONAL INFORMATION FOR THE AUDIT LOG IF NECESSARY.

1.17.6. THE SYSTEM SHALL ALLOW AUTHORISED USERS AND OTHER INDEPENDENT PERSONNEL (E.G. AUDITOR APPOINTED BY THE AUTHORITY) TO VIEW THE AUDIT TRAILS.

1.17.7. THE SYSTEM SHALL ENSURE THAT THESE AUDIT TRAILS BE PROTECTED FROM BEING MODIFIED.

1.17.8. THE CONTRACTOR SHALL ENSURE THE SYSTEM KEEPS THESE LOGS FOR AT LEAST ONE (1) YEAR.

1.17.9. THE SYSTEM SHALL PROMPT AUTHORISED USERS TO ARCHIVE THE AUDIT TRAILS WHEN THE RECORDS REACH OR EXCEED THE RETENTION PERIOD.

- 1.17.10. THE CONTRACTOR SHALL PROVIDE AN ARCHIVAL PLAN SPECIFYING DETAILS ON THE FREQUENCY AND METHOD TO ARCHIVE THE AUDIT TRAILS. THE ARCHIVAL PLAN SHALL BE SUBJECTED TO THE AUTHORITY'S REVIEW AND APPROVAL.
- 1.17.11. THE CONTRACTOR SHALL BE RESPONSIBLE FOR THE ARCHIVAL OF AUDIT TRAILS ACCORDING TO ARCHIVAL PLAN TO BE PROVIDED.
- 1.17.12. THE SYSTEM SHALL ALLOW AUTHORISED USERS TO QUERY THE AUDIT TRAILS, AND PRINT SELECTED PORTIONS OF THE AUDIT TRAILS (E.G. BY A PARTICULAR ACTIVITY OR USER) AS AND WHEN REQUIRED. THE AUDIT TRAILS MUST BE PRESENTED IN A FORMAT THAT IS EASY TO READ BY AUTHORISED USERS.
- 1.17.13. THE CONTRACTOR SHALL ENSURE THAT A PROCESS IS PUT IN PLACE 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 AUTHORITY. WHERE POSSIBLE, AUTOMATED TOOLS MAY BE PROPOSED AS AN OPTION.
- 1.17.14. UPON NOTIFICATION BY THE AUTHORITY OR THE AUTHORITY 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 3 months old	Within ONE (1) day
More than 3 months old	Within FIVE (5) days

TABLE 2: TURNAROUND TIME FOR LOGS

1.18. Security Monitoring and Vulnerability Scanning

- 1.18.1. THE CONTRACTOR SHALL DEVELOP AND MAINTAIN A SECURITY PLAN THAT IS SPECIFIC TO THE SYSTEM, WHICH INCLUDES THE MONITORING OF SECURITY VULNERABILITIES THAT AFFECT THE SYSTEM'S SERVICES, THE ACTIONS THAT NEED TO BE TAKEN TO ADDRESS THE SECURITY VULNERABILITIES, THE TIMELINE AND THE FUNCTION RESPONSIBLE FOR REVIEWING OR TESTING, AUTHORISING AND IMPLEMENTING THE SECURITY PATCHES.
- 1.18.2. THE TENDERER SHALL PROVIDE A DETAILED DESCRIPTION OF THE SECURITY MEASURES AND PROCEDURES TO PREVENT MALICIOUS CODES FROM HARMING THE SYSTEM AND NETWORKS. THE CONTRACTOR SHALL IMPLEMENT SECURITY MEASURES AND APPROPRIATE PROCEDURES TO MINIMISE THE POTENTIAL FOR THE INTRODUCTION OF MALICIOUS SOFTWARE INTO THE SYSTEM AND NETWORK.
- 1.18.3. THE CONTRACTOR SHALL TRANSMIT SECURITY EVENT LOGS OR APPLICATION/DEVICE LOGS IN NEAR REAL-TIME TO THE AUTHORITY'S SUBSCRIBED CYBERWATCH CENTER (CWC) OR SECURITY OPERATIONS CENTER (SOC) FOR OVERALL SITUATION AWARENESS OF THE SYSTEM ICT INFRASTRUCTURE AND SECURITY INCIDENTS IN ACCORDANCE TO REQUIREMENTS SPECIFIED IN THIS TENDER.
-

- 1.18.4. 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 5 MINUTES IN THE EVENT THAT UNAUTHORISED CHANGES HAVE OCCURRED.
- 1.18.5. THE CONTRACTOR SHALL ENSURE THAT LOGS GENERATED FROM ANY SYSTEM MANAGED APPLICATION, DEVICE, OR SYSTEM CAN BE TRANSMITTED TO THE AUTHORITY'S CWC OR SOC IN NEAR REAL-TIME FOR MONITORING PURPOSES.
- 1.18.6. THE CONTRACTOR SHALL MAKE AVAILABLE ALL REQUIRED LOGS FOR SECURITY MONITORING. EXAMPLES OF SOURCES OF SUCH LOGS ARE: —
- (a) Virtual Private Network (VPN) gateways;
 - (b) Domain Name Service (DNS) systems;
 - (c) Firewalls;
 - (d) Network Intrusion Detection/Prevention Systems (NIDPS)/Host Intrusion Detection/Prevention Systems (HIDS);
 - (e) Desktop Security Services applications;
 - (f) Content filtering systems;
 - (g) Web caching systems;
 - (h) Dynamic Host Configuration Protocol (DHCP) systems; and
 - (i) Vulnerability scanners.

1.19. Communication Security

- 1.19.1. ALL INTER-SYSTEM COMMUNICATION (IE COMMUNICATION WITH AN EXTERNAL SYSTEM) CHANNELS (THE TRANSMISSION OF ALL TRANSACTIONS AND DATA TRAFFIC WITH EXTERNAL NETWORKS) SHALL BE PROTECTED USING CHANNEL ENCRYPTION AND MUTUALLY AUTHENTICATED.
- 1.19.2. 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).
- 1.19.3. THE PROPOSED PROTECTION FOR INTRA-SYSTEM AND INTER-SYSTEM COMMUNICATION CHANNELS SHALL LEVERAGE ON THE PROPOSED KEY MANAGEMENT SYSTEM AND SECURE KEY STORAGE (E.G. HARDWARE SECURITY MODULE, TRUSTED PLATFORM MODULE (TPM), SMART CARD OR EQUIVALENT).
-

- 1.19.4. THE PROPOSED SYSTEM SHALL HAVE AN ENCRYPTION SCHEME TO PROTECT SENSITIVE INFORMATION DURING STORAGE (INCLUDING DATABASE) FROM VIEWING AND AUTHORIZING BY UNAUTHORIZED PERSONNEL AND ADMINISTRATOR. THE PROPOSED PROTECTION SHALL LEVERAGE ON THE PROPOSED KEY MANAGEMENT SYSTEM AND SECURE KEY STORAGE (E.G. HSM, TPM, SMART CARD OR EQUIVALENT).
- 1.19.5. FOR ENABLE LOGGING ON ALL SERVERS, FIREWALLS, AND NETWORK COMMUNICATION THAT REQUIRES HIGHER LEVEL OF ASSURANCE,
- a) The Contractor shall propose a One Way Information Flow Gateway for transmission of files between any two physically segregated networks (e.g. between trusted network and any un-trusted networks) by not having direct connectivity across the two networks.
 - b) The One Way Information Flow Gateway shall ensure that all data entering the trusted network are free of malicious content and are in accordance to security policy (i.e. authorised protocol, pre-determined data structure and system-to-system data exchanges).
 - c) The proposed One Way Information Flow Gateway shall ensure that all data exiting from the trusted network are in accordance to security policy (i.e. authorised data, authorised protocol, pre-determined data structure and system-to-system data exchanges).

1.20. Data Exchange Services Security

- 1.20.1. THE DATA EXCHANGE SERVICES SHALL PROTECT THE CONFIDENTIALITY AND INTEGRITY OF ALL INFORMATION WITHIN THE SYSTEM WHEN THE INFORMATION IS IN TRANSMISSION OR AT REST.
- 1.20.2. THE DATA EXCHANGE SERVICES SHALL PROVIDE SECURE TRANSACTIONS TO PROTECT ALL INFORMATION WITHIN THE SYSTEM WHEN THE INFORMATION IS IN TRANSIT. XML ENCRYPTION VERSION 1.1 OR EQUIVALENT RECOGNIZED STANDARD SHALL BE SUPPORTED.
- 1.20.3. THE DATA EXCHANGE SERVICES SHALL BE RESISTANT TO THE FOLLOWING ATTACKS:
- a) XML packet inspection to prevent XML attacks, malformed XML packets
 - b) Fail safe strategy against spoofed identity, weak cryptography, and weak session management.
 - c) Denial of services attacks to prevent broken authentication.
 - d) Broken and/or flawed access control to prevent escalation of privileges.
 - e) The Contractor shall describe if these are provided in the existing Security Gateway solution.

1.21. Backup Security

- 1.21.1. THE PROPOSED BACKUP SOLUTION SHALL ENABLE THE INTEGRITY OF ALL BACKUP DATA TO BE PROTECTED USING STRONG ENCRYPTION WHICH SATISFIES THE REQUIREMENTS OF CRYPTOGRAPHIC CONSIDERATIONS.
- 1.21.2. THE PROPOSED BACKUP SOLUTION SHALL HAVE FEATURES TO ENABLE BACKUP DATA TO MAINTAIN THE SAME INTEGRITY STATE AS THE SOURCE DATA.
-

1.21.3. THE PROPOSED BACKUP SOLUTION SHALL HAVE THE FEATURE TO ENABLE BACKUP DATA TO MAINTAIN THE SAME ACCESS RIGHTS AS THE SOURCE DATA.

1.21.4. THE BACKUP DATA SHALL REMAIN IN ENCRYPTED FORM FOR ALL BACKUP OPERATIONS (E.G. STORAGE)

1.22. Subcontracting and Assignment

1.22.1. THE AWARDED CONTRACTOR SHALL NOT, WITHOUT THE WRITTEN CONSENT OF THE GOVERNMENT, SUBCONTRACT, TRANSFER OR ASSIGN THIS CONTRACT OR ANY PART OF THIS CONTRACT TO ANY PERSON. THE AWARDED CONTRACTOR SHALL BE RESPONSIBLE FOR THE ACTS, DEFAULTS, NEGLIGENCES OR OMISSIONS OF ANY ASSIGNEE OR SUBCONTRACTOR, THEIR AGENTS, SERVANTS OR WORKMEN AS FULLY AS IF THEY WERE THE ACTS, DEFAULTS, NEGLIGENCES OR OMISSIONS OF THE AWARDED CONTRACTOR, HIS AGENTS, SERVANTS OR WORKMEN.

1.22.2. IN SEEKING THE WRITTEN CONSENT OF THE GOVERNMENT, THE AWARDED CONTRACTOR SHALL PROVIDE ALL INFORMATION REQUESTED BY THE GOVERNMENT INCLUDING BUT NOT LIMITED TO INFORMATION ABOUT AN ASSIGNEE'S OR A SUBCONTRACTOR'S REGISTRATION WITH THE RELEVANT GOVERNMENT REGISTRATION AUTHORITY. INFORMATION ON THE GOVERNMENT REGISTRATION AUTHORITY CAN BE FOUND IN <PORTAL> VIA [HTTP://WWW.<PORTAL>.GOV.SG](http://www.<portal>.gov.sg).

1.22.3. IN THE EVENT THAT THE AWARDED CONTRACTOR ASSIGNS OR SUB-CONTRACTS OR TRANSFERS THIS CONTRACT OR ANY PORTION THEREOF WITHOUT THE PRIOR WRITTEN PERMISSION OF THE GOVERNMENT, THE GOVERNMENT (WITHOUT PREJUDICE TO ITS OTHER RIGHTS AND REMEDIES) SHALL HAVE THE RIGHT TO TERMINATE THIS CONTRACT BY WRITTEN NOTICE OF TERMINATION TO THE AWARDED CONTRACTOR AS FROM THE DATE SPECIFIED IN THE NOTICE, AND THE AWARDED CONTRACTOR SHALL HAVE NO CLAIM FOR ANY DAMAGES OR COMPENSATION AGAINST THE GOVERNMENT.

ANNEX I – PRICE SCHEDULE

1. The Contractor shall fill in the Price Schedule based on the attached Excel template.

ANNEX II – FORMAT FOR STATEMENT OF COMPLIANCE

1. The Contractor shall fill in the Statement of Compliance with the following responses to all clauses and sub-clauses of this RFQ.

2. The Contractor shall take note that the response shall take into consideration all annexes referenced. Where there is a failure to indicate any compliance against any clause or sub-clause, the Contractor will be deemed to have indicated "Compliance" and the Quotation will be evaluated accordingly.
3. Only the following responses are acceptable:

"Compliance" or "C"	<p>Able to comply with the requirements. The Contractor shall not add comments against the clause that vary the meaning of full compliance to the clause. However, comments indicating references to literature to substantiate the response is permissible. Any other comments, which will vary the meaning of full compliance, will be ignored</p> <p>For statement that do not call for the Contractor to meet a specific requirement but merely informs the Contractor of a fact, the Contractor's response shall state "C"</p>
"Non-Compliance" or "NC"	<p>Unable to comply with the requirements at all.</p> <p>Explanatory notes must be provided under the column "Remarks" for cases where the compliance is "NC"</p>

Clause Reference	Compliance (C / NC)	Explanatory Notes / Remarks (please include any assumptions made)
1.1		
1.2		
2.1		
2.2		
3.1		
...		
...		
Etc		
[INSTRUCTIONS: Please include all		

clauses from this RFQ]		
------------------------	--	--

ANNEX III – FORMAT FOR CONTRACTOR INFORMATION

Item	Description
1.0	General Information
1.1	Vendor name
1.2	UEN (Unique Entity Number)/ Company/Business Registration No.
1.3	GST Registration No
1.4	Address
1.5	Name of Contact Person
1.6	Telephone number
1.7	Country of incorporation
1.8	Year of establishment
1.9	Areas of specialisation
1.10	Years of involvement in support and maintenance of Microsoft Dynamics AX and applications hosted in GCC.
2.0	Contractor's Staff Profile Relevant to the RFQ
2.1	No. of staff proficient in Microsoft Dynamics AX
2.2	No. of staff familiar with GCC
2.3	No. of staff experienced in managing Grant Management System(s)
(please include other relevant information, if any)	
3.0	Number of Projects Delivered by Contractor, where application is:

2.1	Microsoft Dynamics AX	
2.2	Grant Management System	
(please include other relevant maintenance and support services, if any)		

ANNEX IV – FORMAT FOR CONTRACTOR’S PERSONNEL INFORMATION

Please fill in one copy of the form below for each personnel that will be involved in the project. All personnel shall be subjected to security clearance after the award of the project.

Project Team Personnel Information	
Name	
Nationality	
Current Position	
Years of Work Experience	
Proposed Position for this Project	
Any conflicts of interest to declare?	Yes / No *Delete where applicable
If Yes, please elaborate	
List any relevant support and maintenance experiences with (1) Microsoft Dynamics AX and/or (2) System of similar scale	
Project 1 Name of Project: Project Start and End Date: Nature of Project: Role in Project: Works performed (please list): Relevant Skills and Expertise applied (please list):	

Project 2 Name of Project: Project Start and End Date: Nature of Project: Role in Project: Works performed (please list): Relevant Skills and Expertise applied (please list):	
(please list more projects, if applicable)	

ANNEX V – FORMAT FOR CUSTOMER REFERENCES

Please fill in the customer references based on the tables below whom you had provided maintenance and support for (a) System(s) based on Microsoft Dynamics and (b) System(s) of similar scale hosted in GCC. You may append additional customer references where necessary.

Customer Reference 1 – System based on Microsoft Dynamics AX

Item Description	Information
Customer / Agency Name and Contact Information	
Name and Description of Project	
Project Scope, Vendor Responsibility and Deliverables	
Application version supported	
Hosting Environment	
Project Duration (Indicate Start and End Date)	
Project Cost	
Key members (roles, responsibility)	
Is End User Support services provided?	Yes / No

Additional Information, Comments, or Any Value Added Services	
<please list other information, if applicable>	

Customer Reference 2 – System based on Microsoft Dynamics AX

Item Description	Information
Customer / Agency Name and Contact Information	
Name and Description of Project	
Project Scope, Vendor Responsibility and Deliverables	
Application version supported	
Hosting Environment	
Project Duration (Indicate Start and End Date)	
Project Cost	
Key members (roles, responsibility)	
Is End User Support services provided?	Yes / No
Additional Information, Comments, or Any Value Added Services	
<please list other information, if applicable>	

Customer Reference 3 – System of similar scale hosted in GCC

Item Description	Information
Customer / Agency Name and Contact Information	

Name and Description of Project	
Project Scope, Vendor Responsibility and Deliverables	
Application version supported	
Hosting Environment	
Project Duration (Indicate Start and End Date)	
Project Cost	
Key members (roles, responsibility)	
Is End User Support services provided?	Yes / No
Additional Information, Comments, or Any Value Added Services	
<please list other information, if applicable>	

Customer Reference 4 – System of similar scale hosted in GCC

Item Description	Information
Customer / Agency Name and Contact Information	
Name and Description of Project	
Project Scope, Vendor Responsibility and Deliverables	
Application version supported	
Hosting Environment	
Project Duration (Indicate Start and End Date)	
Project Cost	
Key members (roles, responsibility)	

Is End User Support services provided?	Yes / No
Additional Information, Comments, or Any Value Added Services	
<please list other information, if applicable>	
