PART 2

REQUIREMENT SPECIFICATIONS

Employment and Employability Institute Pte Ltd
80 Jurong East Street 21, #07-03, Singapore 609607
Company Registration No: 200704772C

www.e2i.com.sg | (65) 6474 0606

CONTENTS

CLAUSE NO.

1. INTRODUCTION
2. OBJECTIVES
3. SCOPE OF SERVICES AND DELIVERABLES
4. PROJECT MANAGEMENT
5. PROJECT TIMELINE
6. IMPLEMENTATION PLAN
7. PANEL OF PARTNERS

ANNEXES

ANNEX A: Inventory of Spatial Solutions Deployed at e2i Career Centres

ANNEX B: IT Specifications

1. INTRODUCTION

Employment and Employability Institute Pte Ltd (e2i)

1.1 e2i is a tripartite initiative of the National Trades Union Congress set up to support nationwide manpower and skills upgrading initiatives.

1.2 Please see https://www.e2i.com.sg/ for more information on e2i.

1.3 To date, e2i has 28 Career Centres in Singapore. These centres serve as physical touchpoints for individuals who are seeking employment assistance. To ensure that our centres are appealing to all demographics and to enhance the client experience at our touchpoints, it is essential to employ modern and flexible design principles and leverage newer technology like interactivity and augmented reality for our centres. Through spatial solutions, our goals are to:

1.3.1 Grab attention and drive footfall from incidental traffic;

1.3.2 Foster a comprehensive understanding of e2i;

1.3.3 Provide access to valuable resources that enhances job seekers' employability, job search capabilities and personal growth;

1.3.4 Build a distinct and cohesive brand image;

1.3.5 Ensure that visitors have a memorable experience;

1.3.6 Allow opportunities to share their experiences on social platforms to amplify our reach;

1.3.7 Enhance visitor engagement; and

1.3.8 Leave a lasting impression on our diverse audience.

1.3.9 Refer to Annex A for a list of hardware deployed at existing career centres.

2. OBJECTIVES

2.1 The project is guided by the following principles:

2.1.2 Keeping the total cost of ownership manageable;

2.1.3 Implemented solutions should provide:

(a) Ease of operations;

(b) Ease of scalability;

(c) Ease of maintenance;

(d) Ease of migrations and transitions;

(e) Ease of managing Governance, Risks, and Compliances;

2.1.4 Enhanced capabilities to provide day-to-day operations support and monitoring.

3. SCOPE OF SERVICES AND DELIVERABLES

3.1 The Tenderer shall submit the proposal for all of Clause 3 for a duration of **four (4) years**.

3.2 Infrastructure and Software Development

3.2.1 The proposed solution is to equip e2i touchpoints with suitable technology that can meet present and future needs, surrounding the following considerations:

(a) Allowances for high scalability and agility to meet evolving business needs and growth;

(b) Stability of the overall infrastructure in enabling high availability;

(c) Allowances for interactable functionalities (e.g., Programmes that are touch enabled or leverage Augmented Reality, etc.)

3.2.2 The proposed solution is to incorporate the following:

(a) Hardware;

(b) Software; and

(c) Additional functionality and requirements

3.2.3 Hardware

The Tenderer shall propose hardware requirements for the proposed solution. The proposal shall include the following:

(a) Type and specifications of hardware;

(b) Quantity of mentioned hardware;

(c) Purpose of mentioned hardware;

(d) Installation and deployment of mentioned hardware, infrastructure, housing, and peripherals;

(e) Maintenance of mentioned hardware; and

(f) Any other requirements not listed above.

3.2.4 Software

The Tenderer shall propose software requirements for the proposed solution. The proposal shall include the following:

(a) Design and development of software(s) or application(s);
(b) Functionalities of mentioned software(s) or application(s);
(c) User journey for the use of mentioned software(s) or application(s);
(d) Scalability of mentioned software(s) or application(s);
(e) Post-implementation maintenance of mentioned software(s) or application(s); and
(f) Any other requirements not listed above.

For any software(s), the Tenderer shall ensure that the environment in which the software(s) is/are hosted shall be minimally ISO27001 certified.

3.2.5 Additional Functionality and Requirements

(a) The Tenderer shall detail any additional functionality and requirements as part of the proposed solution that is not listed in Sub-Clause 3.2.3 and 3.2.4. These additional requirements can include but are not limited to, WiFi system, server, storage, cloud infrastructure, and maintenance.

(b) For each additional requirement, the Tenderer shall minimally include the purpose and cost of the additional requirements.

3.3 Spatial Design

3.3.1 The Tenderer shall propose spatial design elements for the proposed solution. The proposal shall include the following:

(a) Concept of the spatial design;
(b) Key features of the said spatial design;
(c) User journey for the said spatial design; and
(d) Any other requirements not listed above.

3.3.2 The Tenderer shall detail any additional functionality and requirements to support the proposed solution that is not listed in Sub-Clause 3.3. These additional requirements can include but are not limited to, Content Management System and maintenance.

3.3.3 For each additional requirement, the Tenderer shall minimally include the purpose and cost of the additional requirements.

3.4 Other Requirements

3.4.1 The Tenderer shall include in the proposal, where relevant:

(a) Compliance with ISO and e2i's ISO policies;
(b) Any proposed IaaS shall be CIS compliant;
(c) Compliance with IT Specifications (see Annex B);
(d) Maintenance, subscriptions and management of the solution post-implementation; and
(e) Options to extend maintenance, warranty and services to the fourth year.

3.5 Key Performance Indicators

The Tenderer shall ensure the following are included in the proposal:

(a) Suitable indicators to measure user responses and effectiveness of the solutions proposed; and
(b) Indicator data can be measured and obtained readily.

3.6 Professional Services

3.6.1 Hardware Deployment – The Tenderer shall include the following during deployment:

(a) Hardware staging and onsite mounting;
(b) Physical cabling of both power and network connectivity.

3.6.2 Infrastructure Implementation – Solutions deliverables based on Clause 3.2 to 3.3.

3.6.3 Documentation – Documentation for the project shall include, but not be limited to, clauses listed in Annex B.

3.6.4 Training – The Tenderer shall ensure sufficient training is provided to e2i-nominated personnel in the management and use of the solutions proposed. The Tenderer shall provide the following:

(a) Training proposal; and
(b) Training course and materials.

3.7 Tender Response Scenarios

3.7.1 As part of the Tender Proposal, the Tenderer shall provide a written response to each of the hypothetical scenarios set out in Clauses 3.7.4 to 3.7.6.

3.7.2 The scenarios are provided for the purpose of allowing e2i to understand the Tenderer's proposed approach, methodology and capability in delivering the Services. The scenarios are illustrative and are not intended to represent an exhaustive description of the situations that may arise during the Contract Period.

3.7.3 In responding to each scenario, the Tenderer may state any reasonable assumptions made and may recommend alternative approaches where the Tenderer considers such alternatives appropriate.

3.7.4 Scenario 1: Maintenance of Existing Spatial Assets

Assume that the Tenderer has taken over the maintenance and support of e2i's existing spatial assets deployed across its Career Centres, including the relevant hardware and software.

The Tenderer shall describe its proposed approach to maintaining the assets in good working condition throughout the Contract Period.

The Tenderer's response should set out its proposed maintenance approach, including any preventive maintenance, inspection, monitoring, servicing, record-keeping and asset-management practices that the Tenderer considers appropriate.

3.7.5 Scenario 2: Fault Diagnosis, Troubleshooting and Rectification

Assume that a spatial asset deployed at an e2i Career Centre experiences a hardware failure, software fault or other technical issue that affects its normal operation.

The Tenderer shall describe how the Tenderer would manage the incident from notification or detection through to resolution and closure.

The Tenderer's response should describe its proposed approach to:

(a) identifying and diagnosing the fault;
(b) assessing the impact and severity of the incident;
(c) notifying and updating e2i;
(d) troubleshooting and rectifying the fault;
(e) determining whether the affected asset should be repaired, replaced or otherwise restored;
(f) managing the expected response and resolution timeframe; and
(g) documenting the cause, actions taken and final resolution.

Where applicable, the Tenderer's proposed approach shall be consistent with the relevant incident severity, response, resolution and escalation requirements stipulated in Annex B.

3.7.6 Scenario 3: Identification and Proposal of New Spatial Solutions

Assume that, during the Contract Period, e2i identifies a new or existing Career Centre where a spatial solution may be required to support its operational, engagement or communication needs.
The Tenderer shall describe how it would work with e2i to assess the requirements and identify, recommend and implement an appropriate spatial solution.
The Tenderer's response should describe its proposed approach to:

(a) understanding the operational, user and site requirements;
(b) assessing the physical space and existing infrastructure;
(c) identifying suitable technologies and spatial solutions;
(d) evaluating the feasibility, scalability, maintainability and integration requirements of the proposed solution;
(e) presenting appropriate solution options and recommendations to e2i;
(f) providing indicative implementation requirements, timelines and costs; and
(g) implementing the approved solution, where subsequently instructed by e2i.

4. PROJECT MANAGEMENT

4.1 e2i's Representative

e2i shall appoint a person to supervise and liaise with the Tenderer for the purpose of the Contract and such person may designate others to assist him/her in such matters.

4.2 Project Organisation

4.2.1 The Tenderer shall appoint an Account Manager who shall oversee the requirements gathering and be the Single Point of Contact.

4.2.2 The Tenderer shall, as part of the overall detailed implementation plan, submit a detailed Account Servicing Team ("AST") structure and working process, taking into consideration the following:

(a) The AST members who work on the pitch and present at face-to-face tender presentation and clarification sessions (if any), **must** eventually work on the e2i's account if the tenderer has been appointed.

(b) If any proposed team member for this Contract will concurrently be working on another account, this information must be stated clearly in the AST structure. Team members dedicated solely to this contract are preferred.

4.2.3 The AST must comprise at least one proposed team member for each of the following roles:

(a) Account Director

Preferably ten (10) years' experience related to spatial and/or experiential design or more

(b) Account Manager
Preferably five (5) years' experience related to spatial and/or experiential design or more

(c) Developer
Preferably three (3) years' experience or more

Assigned personnel for (a) Account Director will be assessed for their number of years of experience, whether they have been directly responsible for projects of similar scale and nature in the past 5 years as part of the evaluation criteria.

4.2.4 The Tenderer shall also indicate the total number of assigned members listed according to the individual parts of this Tender.

4.2.5 An organisation chart of the AST, showing names, reporting lines and key responsibilities shall be included as well.

4.2.6 An implementation plan shall be provided to the e2i to detail the milestones and any contingency plans that is necessary to ensure critical timelines are not compromised.

4.2.7 The Account Manager shall be the key contact person regardless of the specifically assigned members to the e2i. This person shall work full time on the contract and remain contactable at all reasonable times.

4.2.8 The Tenderer shall be ready to accept the e2i's request to provide qualified replacements in the absence of the assigned AST members as submitted for this contract to ensure the effective delivery of all goods and services according to the Tender.

4.2.9 e2i reserves the right to interview the proposed AST team members.

4.2.10 The Account Manager shall ensure that the deliverables are in accordance with the specifications stated in the Contract and completed on schedule. He/she shall take full responsibility for the quality of work produced by his/her team. If the performance of the Account Manager is below expectations, e2i shall escalate to the Tenderer for necessary action.

4.2.11 The Account Manager is required to participate in all the reviews with e2i. Reviews of each milestone shall be incorporated at suitable junctures throughout the Contract.

4.2.12 Minutes of all project meetings shall be recorded by the Account Manager and disseminated to all members of the meeting **within three (3) working days** after the meeting.

4.2.13 The Tenderer's key personnel shall be contactable at all reasonable times via mobile phone and be prepared to be activated after office hours to resolve critical problems.

5. PROJECT TIMELINE

5.1 As part of its Tender Proposal, the Tenderer is required to submit a detailed project timeline. The proposed timeline shall be aligned with, and shall not exceed, the key project milestones stipulated below.

No	Milestones	Date
1	Kickoff meeting and implementation plan	Within 2 weeks from the Effective Date
2	Stock take existing inventory	Within 3 weeks from the Effective Date
3	Takeover existing inventory from incumbent contractor	Within 5 weeks from the Effective Date

5.2 The Tenderer may propose a project timeline where the milestones can be achieved earlier.

6. IMPLEMENTATION PLAN

6.1 The successful Tenderer shall submit an Implementation Plan, **within 2 weeks** from the issuance of the Letter of Acceptance, in accordance with Clause 7.3 of Conditions of Contract.

6.2 In the event of any inconsistency between the details set out in the Implementation Plan and the Project Timeline, the Implementation Plan shall prevail.

7. PANEL OF PARTNERS

7.1 The Tenderer shall provide information of partner/s not listed as members of the consortium with respect to:

7.1.1 Credentials of partner/s

7.1.2 Roles and responsibilities of partner/s

7.1.3 Confirmation of partner's availability and support during contract duration

ANNEX A: Inventory of Spatial Solutions Deployed at e2i Career Centres

e2i Career Centre	Item Description	Quantity
One Marina Boulevard (OMB) 1 Marina Boulevard, #B1-03, Singapore 018989		
OMB	LED Wall (3.08m x 2.95m) + Processor	1
OMB	Media Processor	1
OMB	PC (Tower PC)	1
OMB	Touchscreen Display (43 inch)	3
OMB	PC (Mini PC)	3
OMB	Mobile Data Subscription + SIM Router	1
Our Tampines Hub (OTH) ServiceSG Centre Our Tampines Hub, 1 Tampines Walk, #01-21, Singapore 528523		
OTH	Standard Display (Non-Touch) 65 inch	1
OTH	PC (Mini PC)	1
AMK HUB **S**erviceSG Centre@AMK Hub, 53 Ang Mo Kio Ave 3, #04-02, Singapore 569933		
AMK HUB	Standard Display (Non-Touch) 86 inch	2
AMK HUB	PC (Mini PC)	2
AMK HUB	Mobile Data Subscription + SIM Router	1

ANNEX B: IT Specifications

1. SCOPE OF WORKS

1.1. The Tenderer shall provide the following base scope of work:

(a) Project Management with weekly progress updates

(b) Requirement study

(c) Detailed design

(d) Development and customization

(e) Hosting

(f) Installation and configuration

(g) System testing

(h) User acceptance testing (with UAT test cases)

(i) Vulnerability Assessment and Penetration Test (VAPT)

(j) Data migration

(k) Training for system administrators and end users

(l) Documentation

(m) Performance Guarantee Period (PGP)

(n) System Warranty

1.2. REQUIREMENT STUDY

1.2.1. The Tenderer shall include a detailed requirements study within the implementation plan to understand and validate the business requirements and information/data requirements.

1.2.2. The business requirements, the scope of the information/data requirements, and the number of interfaces shall be documented, reviewed, and signed-off by e2i.

1.2.3. The Tenderer shall leverage on the available technologies that can be quickly and easily implemented to ensure a shorter development period and achieve quicker rollout.

1.2.4. The Tenderer shall contribute their knowledge and experience in similar projects when designing the System.

1.2.5. The Tenderer shall take into consideration of minor adaptations which may need to be implemented without any additional cost during implementation.

1.2.6. The Tenderer shall assist in the review of existing processes and recommend changes to streamline processes where appropriate. Where appropriate, the Tenderer shall propose

areas where e2i should consolidate that will result in better efficiency or cost savings. The Tenderer shall advise the users the requirements and implications for considerations.

1.3. The successful Tenderer shall carry out: -

(a) To conduct a technical analysis to understand and analyse the existing network infrastructure to be used for the implementation of the System.

(b) Design, develop, supply, deliver, install, test, commission and support the System, including all system software, application software, hardware and accessories that are required to support the proper functioning of the System.

(c) Provide a comprehensive change management and training plan and materials to carry out System training for the users and administrators.

(d) Provide maintenance and support during the performance guarantee period and system warranty period as part of the contract, in particular 2nd level helpdesk and single point of contact.

(e) Coordinate with all parties required, to ensure the System's smooth deployment and operation. Overall performance and reliability shall continue to meet prescribed standards at all times.

(f) Provide the fixed man-day rates for raising Change Request to change the System or additional services required during the development and maintenance phases.

(g) Provide the system documents as listed in Clause 11.

(h) Provide and execute user acceptance (with UAT Test cases) and system testing plan for the System.

1.4. The successful Tenderer shall appoint a Project Manager who shall be the single point of contact for the project. The Project Manager shall provide a detailed project schedule that can meet the milestones. The project schedule shall show details of the milestones.

1.5. The successful Tenderer shall coordinate with all parties required, to provide the following scope of works:

(a) To prepare and document the overall application architecture, including the interfaces with other systems and shall conduct a detailed design review with the e2i project team before the commencement of development.

(b) To co-ordinate with the e2i project team in setting up, testing, and maintaining the System.

(c) To provide all installation, backup and recovery procedures for the System.

(d) To train and handover to the Tenderer who is taking over the application maintenance and support in due course if the maintenance of the system and support to the users is awarded to a different Tenderer.

1.6. The Tenderer shall gather the reporting requirement during the Requirement Study phase and shall provide the services for the delivery of all the reports as mutually agreed.

2. PROJECT MANAGEMENT

2.1. PROJECT ORGANISATION

2.1.1. The Tenderer shall, as part of the overall detailed implementation plan, submit a detailed project organization structure clearly specifying the duties and responsibilities of all the personnel assigned to the Contract. Curriculum Vitae of all personnel shall be provided.

2.1.2. The successful Tenderer shall not change the personnel in the project team without prior approval by e2i appointed representatives.

2.1.3. The Tenderer's proposed project team shall comprise of one (1) Project Manager with at the least the following knowledge and experience:

(a) Shall have at least five (5) years of project management experience, of which at least last three (3) years in outsourcing management and be based in Singapore.

(b) Planning and management skills

(c) Excellent interpersonal skills and able to work with people at different levels

(d) Good communication skills in English

(e) Be conversant with the methodology the Tenderer is adopting for deployment

(f) Be conversant with the products and services that the Tenderer is offering including knowledge in the hardware, software, network and mobile connectivity.

(g) Be Singapore Computer Society CITPM and COMIT or PMP certified

2.1.4. The Tenderer shall monitor and effectively manage any sub-contractor(s) that has been selected in the discharge of their duties to meet the requirements established. All matters that require interface between the sub-contractor(s) shall be co-ordinated by the Tenderer to ensure harmony in the relationship among all parties concerned and to establish a common understanding of e2's requirements.

2.1.5. The e2i may engage other contractor to undertake works related to or supply hardware and software intended to integrate with the System. The Tenderer shall co-operate fully with all such contractor to ensure proper integration and interoperability of the System with the works, hardware, and software.

2.1.6. The Tenderer shall ensure that the deliverables are in accordance with the specifications stated for each project and completed on schedule.

2.2. PROJECT MANAGER

2.2.1. The Tenderer's Project Manager shall be responsible for managing the development, deployment, maintenance and operations of the System. This Project Manager shall be the single point of contact between e2i and the Tenderer's project team. In the Project Manager's absence period, a secondary Project Manager, with similar work knowledge and experience stated in Clause 2.1.3, will be appointed to be the single point of contact. There must always be always a Project Manager available at any point of time.

2.2.2. If the performance of the Project Manager is below expectations, e2i shall escalate to the Tenderer's appropriate higher management for necessary action to replace the Project Manager.

2.2.3. The Project Manager shall ensure that the deliverables are in accordance with the specifications stated in the Contract and completed on schedule. He/she shall undertake full responsibility for the quality of work produced by his team and the sub- contractor(s). This includes ensuring that there is consistency and uniformity in the different work produced by his team and the sub-contractor(s).

2.2.4. The Project Manager is required to participate in all the reviews with e2i at location to be decided by e2i. Reviews of each milestone shall be incorporated at suitable junctures throughout the Contract. The Project Manager shall attend all reviews with e2i.

2.2.5. Minutes of all project meetings shall be recorded and disseminated to all members of the meeting within three (3) working days after the meeting.

2.2.6. The Project Manager shall ensure that security is observed by the Tenderer staff in accordance with e2i security policies.

2.2.7. The Project Manager shall maintain records of all development and maintenance activities including proper accounting and administrative records of all services performed during the Contract Period.

2.3. PROGRESS REPORTING

2.3.1. The Project Manager shall submit progress report by the third (3rd) working day of each calendar month for the duration of the Contract. The format of the progress report shall be submitted by the Tenderer for approval by e2i.

2.3.2. The report shall cover:

(a) Updated project schedule vs. baseline project schedule.

(b) Status of all tasks and tasks planned for the next month; problems encountered and envisaged, and recommendations on how to resolve them.

(c) Reasons for any delay(s) and the impact.

(d) Highlight of changes in project scope.

(e) Details of changes; and

(f) Any other details requested by e2i.

2.3.3. The Project Manager may be required to produce ad-hoc progress reports requested by e2i. The submission and acceptance of progress reports shall not in any way prejudice the rights of e2i to make any claims against the Tenderer.

2.3.4. The Project Manager shall produce management reports, which include monthly status reports of all problems reported and queries raised. Some examples are, information of the date problem is reported, date problem is resolved, status of problem, cause of the problem and details on the problem and corrective action taken shall be included. Summary report on the Tenderer service performance shall also be provided.

2.3.5. The Project Manager shall be responsible for informing e2i, as early as possible, 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 Project Manager on the alternatives available.

2.3.6. The Project Manager shall be responsible for establishing the time and agenda, as well as arranging for each progress meeting in view of the milestones achieved. The project manager shall be prepared for each progress meeting with the necessary details for discussion. The

project manager shall also ensure that all relevant personnel from the Tenderer shall be prepared for the meeting.

2.4. PROGRESS REVIEW

2.4.1. In addition to the monthly progress reviews that shall be conducted by the Tenderer, e2i may call progress meetings at regular fortnightly intervals during which the Tenderer's Project Manager shall attend and report to the Management Team on the progress of the services. The progress meetings shall be held at venues chosen by the Management Team.

2.4.2. Reviews of each milestone shall be incorporated at appropriate junctures throughout the course of the project. The Project Manager shall participate in all reviews with the e2i at location to be decided by the e2i. If the Project Manager is not available, he shall be duly represented by a person of higher authority and who shall have good knowledge of the project status and issues. Such representations must be formally communicated to the e2i and must be agreed upon by the e2i prior to the review meeting.

2.4.3. The Tenderer shall provide e2i with a schedule of the technical reviews to be performed on the system design. The technical reviews are to be carried out to ensure the following:

(a) Completeness of interfaces between the System and the external application systems.

(b) Robustness of the application infrastructure and system architecture; and

(c) Technical requirements of the System stated in Requirement Specifications have been met.

2.5. DETAILS OF PROPOSED SUB-CONTRACTOR(S)

2.5.1. Where sub-contractor(s) are proposed, the Tenderer shall furnish the following information as a separate attachment to his Tender submission information as a separate attachment to his Tender submission information as a separate attachment to his Tender submission:

(a) Sub-contractor(s)

(b) Name of Sub-contractor(s)

(c) Email, Address and Telephone Numbers

(d) Names, Age and Qualification of Directors/Partners

(e) Number of employees in the firm

(f) Related Experience of each member

2.5.2. A tender delivered without the names of the proposed sub-contractor(s), whatever the reason may be, shall not be considered. e2i is entitled to request the Tenderer to change the submitted sub-contractor without the need to give any reasons.

2.5.3. All sub-contractor(s) are subjected to e2's approval.

2.6. MOBILISATION / REPLACEMENT OF KEY PERSONNEL

2.6.1. The Tenderer shall not initiate changes in key personnel throughout the Contract without agreement from e2i.

2.6.2. In the event of a need for replacement of key Tenderer personnel, The Tenderer shall seek approval from e2i in writing at least one (1) calendar month prior to the date of replacement, indicating the personnel who shall be assuming the responsibilities concerned. e2i reserves the right to accept or reject the proposed replacement personnel.

2.6.3. e2i reserves the right to require the Tenderer to replace the Tenderer's Project Manager and development/maintenance team members if e2i deems the Tenderer appointed personnel for the roles to be inappropriate. The Tenderer shall provide replacement personnel within two (2) calendar weeks of notice from e2i for such replacement. All Tenderer's commitment in terms of project schedule and deliverable shall continue to apply.

2.6.4. The Tenderer shall be responsible for training the successor to be technically competent to carry out the work. The replacement personnel shall be available for at least a reasonable period (duration to be stipulated by e2i) for the existing personnel to hand-over his responsibilities and duties. The cost incurred for the provision of the replacement personnel during the handing over period shall be borne by the Tenderer.

2.6.5. The Tenderer's Project Manager must supply evidence to the e2i's Representative that the project handover is duly completed before releasing the personnel.

2.6.6. The e2i's Project Handover Procedure must be adhered. Where alternatives are proposed by the Tenderer, the procedure must be approved by the e2i.

2.6.7. The scope of the handover plan, for any types of handover, shall include the following:

(a) Processes and procedures

(b) Roles and responsibilities

(c) Schedule Plan

(d) Outstanding requests/activities

2.7. PROJECT MANAGEMENT PLAN

2.7.1. The Tenderer shall produce and maintain detailed Project Management Plan where applicable showing the proposed development, delivery, installation, testing and implementation strategies and the dates of all major milestones. The Tenderer shall take into consideration project deadlines stipulated by the e2i.

2.7.2. The Tenderer shall update Project Management Plan to reflect planned and actual completion dates. All revised Project Management Plan shall be subjected to e2i's approval.

2.7.3. The Project Management Plan shall include activities to be carried out by the e2i as well as all other personnel whose actions are required. The Project Management Plan shall include a diagram depicting the reporting structure and the key personnel who shall be involved in the project. It shall clearly define the roles and responsibilities of all personnel assigned by the Tenderer to the project and how each project team interacts with one another to deliver the desired Services.

2.8. CO-EXISTENCE STRATEGY

2.8.1. In the event that the e2i appoints more than one Tenderer whether in this tender or subsequent tenders, the Tenderer shall co-operate with each other to ensure that the Service Levels are met. If necessary, the operation management procedures shall have to be refined by all parties to accommodate each other's systems.

2.8.2. The Tenderer, together with the e2i's Representative and the existing e2i's Contractor(s), shall meet as often as required to discuss the operation issues and other problems that may be encountered in the provision of the services. The relevant technical managers or officers involved in the provision of the services shall attend the meetings.

3. SYSTEM REQUIREMENT

3.1. The Tenderer shall propose all the hardware and software (Overall system configurations) to support the complete System requirements. The Tenderer shall specify clearly, the purpose of all the hardware and software components proposed, as well as its available features and associated benefits.

3.2. The Tenderer shall propose the operating systems and system software that operate on Tenderer proposed platform.

3.3. If the functions of the System are leveraging on a third-party software/service, it shall be designed such that changes, or replacement of the third-party software/services shall not require any code change to the System.

3.4. The System shall adopt a 3-tier architecture and application design principles, which helps enforce the logical separation of functionality, such as keeping the data, business logic and presentation layers separate from each other.

3.5. The System shall provide easily accessible online help facilities to the users. The online help shall be provided at the transaction level and screen level. Help facilities shall be context-sensitive and include information to assist users in navigating the System.

3.6. Data validation and computation that require back-end information shall be performed at the Application tier. The business logic at the Application tier shall be component-based and object- based to allow reusability and scalability. On the other hand, independent form data validation and computation could be performed at the Client tier through client-side scripts.

3.7. The System design shall allow scaling and changing each layer with minimum impact on the other layers as requirements and technology changes, thus providing improved scalability, manageability, and resource utilization.

3.8. The design of the System shall incorporate the following characteristics:

(a) Accessibility Provide the right data to the right person at the right time.

(b) Extendibility Extend the scope of the functionality with minimal impact to the existing systems.

(c) Flexibility Respond quickly to changing business needs with minimal rework.

(d) Interoperability Integrate with other internal and external systems with minimal changes.

(e) Manageability Easy to configure and operate in a production environment.

(f) Performance Provide high throughput / responsiveness while balancing cost of service.

(g) Reliability Provide availability and responsiveness to meet designed service levels.

(h) Reusability Leverage functionality with minimal rework or impacts on other systems.

(i) Scalability Handle the increased volumes of transactions and data with minimal impact on performance

(j) Security Control access to functions and data without restricting ease of use

(k) Electronic Data Entry Wherever possible and existing electronic data banks are available, data shall be electronically captured without tedious re-entries.

(l) Software Portability All application software shall be in highly portable codes so that it can be transferred easily from one computer system to another. For example, the systems can be accessible via different platforms, different browsers and different devices.

(m) Hidden Functionalities The application developed shall not contain any hidden functionalities which e2i is not made aware of.

(n) Transparency The application developed shall be transparent in its processing logics so that users are able to identify a data or usage error.

(o) Auditability The application developed shall allow for audit logs of key transactions.

3.9. The Tenderer shall seek permission from e2i whenever a system downtime is required.

3.10. The Tenderer shall ensure that the design of the physical and logical databases is optimum and establish efficient and effective access of the database to the System. The physical and logical database documentation, including the data modelling and entity relationship, shall be provided and maintained updated.

3.11. The proposed System shall have function to purge personal data older than the stipulated data retention period as defined by e2i. However, the System shall archive demographical data for aging purposes.

3.12. GRAPHICAL USER INTERFACE (GUI)

3.12.1. The System shall provide a mobile and user-friendly and intuitive graphical interface (GUI) with easy-to-use online help.

3.12.2. The System shall have the following GUI features:

(a) Menus shall be structurally arranged and each option in the menu shall be easily accessible.

(b) Use of pictures and icons that are meaningful and highly intuitive to the users.

(c) Descriptive labels and control buttons names shall accurately genuinely convey their intended behavior.

(d) Grouping of related tasks to reduce overall complexity; and

(e) Keystrokes for operation of the System shall be minimized.

(f) Process driven to guide users achieve the purpose of the online transaction.

3.12.3. The Tenderer shall ensure that all error messages shall be descriptive enough for users to perform corrective actions.

3.12.4. The Tenderer shall provide online help facilities at appropriate points to assist users.

3.13. EXCEPTIONAL HANDLING

3.13.1. The System shall provide necessary error messages for troubleshooting. Error messages should describe the problem in simple terms that is easy to understand by users.

3.13.2. The System shall perform proper error handling. A hierarchy of error levels, codes, and messages should be developed for each application modules. Error messages should be stored in common storage. There should be error codes corresponding to error messages so that it is easier to modify the messages without code modification.

3.13.3. Errors should be classified into severity levels, such as “warning”, “input error” and “fatal error”.

3.13.4. In the event of a serious error defined in the Severity Levels, the System shall perform recovery to ensure continued execution, or degrading gracefully to prevent abrupt end to any session/process.

3.13.5. The System shall allow for manual intervention to handle exception, errors, and some changes to the business workflow.

3.14. SYSTEM ROLES AND RESPONSIBILITY MATRIX

3.14.1. The Tenderer shall work with e2i to setup an authorization matrix for Access Roles segregation, after studying e2i’s key business processes and requirements. The authorization matrix shall define roles and responsibilities and assign proper access to each user of the System. The roles and responsibilities listed below are not exhaustive and the Tenderer shall work with various stakeholders to define and confirm the authorization matrix. The authorization matrix shall be documented for references.

3.14.2. The Tenderer shall refer to the respective System modules to review the different access levels and user roles for each module and may propose and provide an authorization matrix which best suit our business needs and requirements. However, such proposal shall be subjected to review and approval by e2i.

3.14.3. The Tenderer shall build the capability for users to schedule auto-generated reports of all user lists, user group lists and user access matrix based on frequency and list of recipients.

3.15. SYSTEM INTERFACE REQUIREMENTS

3.15.1. The Tenderer shall provide the implementation services for the delivery of the system interfaces based on the requirements specified in this tender specification.

3.15.2. The System interfaces shall be via web service, batch and/or file upload. All interfaces shall be in compliance with e2's policies.

3.15.3. The System shall have open Application Programming Interface (API) capability, to allow future interfaces or integrations with other systems. Any integration works that The Tenderer tap on from their existing API libraries shall not be chargeable to e2i.

3.15.4. The design of the System interfaces shall ensure new connections to other systems can be easily added, obsolete connections can be easily removed, and protocols and format of existing connections can be modified with minimum disruption to operations.

3.15.5. The Tenderer shall describe in detail how the interfaces can be made robust enough to guard against possible unsuccessful data transfer/data loss/corruption, error handling as well as the detection and recovery from such occurrences.

3.15.6. The Tenderer shall ensure that all data extraction from the System, data updates to the System and file exchanges are automated and logged, with prompt alerts to authorised personnel, in cases of unsuccessful execution of the system interface in the System's production environment.

3.16. GROWTH AND FUTURE REQUIREMENT

3.16.1. The Tenderer shall ensure that the proposed hardware sizing and configuration and system software are scalable and upgradeable, and the design of the System is modular/flexible to cater for future growth and expansion in the following areas without having to replace the hardware, operating system or requiring major re- design of the System:

(a) Twenty percent (20%) annual growth in the full System workload over the life span of the System.

(b) Additional Hardware units to be included easily without much modification to the Hardware, Software and network configurations

(c) Foreseeable organisational changes and procedural changes.

3.16.2. The Tenderer shall provide a clear and comprehensive technology upgrade paths for the System hardware and software.

3.17. HOSTING REQUIREMENTS

3.17.1. The Tenderer shall provide a cloud hosting environment on a dedicated logically isolated and scalable cloud infrastructure, hosted in Singapore region.

3.17.2. The hosting environment should have the following:

(a) Meet Multi-Tier Cloud Security (MTCS) Singapore Standard (SS) 584 cloud security level 3 certification.

(b) Encrypt all data in transit with 256-bit Advanced Encryption Standard (AES).

(c) Meet system availability service level agreement as per tender specification.

3.17.3. The Tenderer shall provide two environments: Production and User Acceptance Test (UAT). Development environment is at the Tenderer own cost.

3.17.4. The Tenderer shall propose the sizing for all the resources that will be configured in the cloud or any resources outside of cloud based on the application requirements.

3.17.5. The Tenderer shall make provision to ensure that any proposed cloud computing and software capabilities are open and flexible to meet future technology changes that may provide better performance and scalability. In the event that the cloud service provider releases and upgrade its services to provide a more cost-efficient solution, Tenderer shall assist to upgrade/migrate the solution to the new cost-efficient solution at no additional cost to e2i e.g. moving of cloud servers to upgraded compute instances that offer better performance at better price.

3.17.6. Licensed Anti-virus software, including license renewal, shall be deployed to all virtual machines in the hosting environment.

3.17.7. The Tenderer shall ensure both the Production and UAT environment have the same level of IT security.

3.17.8. The Tenderer shall provide SMTP services to send and receive emails for the system.

3.17.9. The Tenderer shall configure the alerts to send out via SMS / emails to e2i if the system or hosting services is down.

3.17.10. The Tenderer shall provide a single point of contact (POC) based in Singapore. For the technical support personnel, he / she should be based in the same time zone (GMT+8) and be always contactable via mobile phone.

3.17.11. The Tenderer shall quote the hosting cost in the tender proposal.

4. TECHNICAL REQUIREMENT

4.1. GENERAL REQUIREMENTS

4.1.1. The System shall be proven in design and operation, and able to meet the stipulated load and performance.

4.1.2. The System shall be designed to separate heavy duty reports generation from transactional system.

4.1.3. The System shall have housekeeping and archival features.

4.1.4. The Tenderer shall provide a logical diagram on the proposed hardware and any additional components and their connectivity to e2i's infrastructure.

4.1.5. The Tenderer shall ensure the System is design, developed and configured with good performance, maintainability, reliability, availability, and security controls. This is to ensure that it does not affect the data availability, integrity, confidentiality and performance of other applications hosted in the common infrastructure.

4.1.6. The Tenderer shall provide and install any plug-in / software required to run the System on the Workstation laptop and the mobile phones/tablets and ensure that the plug-ins do not interfere with the running of the existing software on the laptops. The plug-in / software should not behave in a worm-like behavior that may trigger a false alarm for e2i's security defense mechanisms.

4.1.7. The Tenderer shall supply information on the programming language(s), compiler(s) and editor(s) used for the System.

4.1.8. The Tenderer shall advise on all matters relating to the installation, configuration, operation and performance tuning of the System.

4.2. INTERFACE AND SECURITY REQUIREMENTS

4.2.1. The System shall comply with all e2's IT Security Policy, Standards and security requirement checklists. The security requirement details shall be made available only to The Tenderer.

4.2.2. The System shall use Secured Shell (SSH) technology to perform secure file transfer (SFTP).

4.2.3. The System shall use Secured Socket Layer (SSL) for application layer encryption.

4.2.4. The System shall comply with e2i's Password Policy and provide the interface tomodify the password parameters without modifying the program codes.

4.2.5. As the System collects personal data, the Tenderer is required to comply to the Data Privacy Act. The Tenderer shall ensure compliance should there be further changes required by the programme or the above-mentioned acts. Please refer to official website for latest update and detailed info: https://www.pdpc.gov.sg

4.3. BACKUP AND RECOVERY REQUIREMENTS

4.3.1. The Tenderer shall work with e2i and third (3rd) party maintenance contractor if the maintenance and support service is awarded to a different contractor, to provide a backup and recovery process and facilitate the recovery of all transactions and data up to the last successful transaction before a system failure occurs.

4.3.2. In the event that the maintenance and support service is awarded, the Tenderer shall define and implement a comprehensive Backup and Recovery Plan for the deployment of the System. The Backup and Recovery Plan shall ensure that the backup and recovery process recover all transactions and data up to the last successful transaction before the System failure occurred. The Plan to be prepared shall at least include information such as data retention periods, frequency of backup, types of backups (such as incremental and full back up), what data to backup (such as application data files, system files), and the process of system recovery from the backups following a system failure and fallback procedures.

4.3.3. The backup and recovery plan shall include the following areas:

(a) Overview of the backup strategy

(b) Time and Resources required for backup of reach of the transactions

(c) Detailed backup procedure

(d) Time and Resources required for recovery for each of the transactions

(e) Detailed recovery procedure

(f) Housekeeping tasks

4.3.4. The Tenderer shall ensure that the backup process/operation is not run during the Support Hours in any month and shall not affect the performance of the System.

4.3.5. The Tenderer shall perform annual restoration of the backup as well as a monthly report of the backup status.

4.3.6. The Tenderer shall ensure that the System continues to operate during the period when back-up activities are running.

4.3.7. If the backups are hosted on cloud, the backup system must be maintained by a different provider. Processes and procedures shall be taken to ensure that the backup is not hosted on the same PaaS/IaaS infrastructure as the primary data.

(a) 14 days of back up must be maintained

(b) With a 24-hour recovery point objective (RPO)

(c) And a 24-hour recovery time objective (RTO) Note: Backups hosted on a different cloud infrastructure but managed by the same vendors meet this requirement. For e.g., a cloud storage vendor maintains an encrypted content backup on AWS.

4.4. ARCHIVAL AND HOUSEKEEP

4.4.1. The System shall have the following features for housekeeping:

(a) Facility to archive historical data which shall be on a user-specified periodic batch basis.

(b) Facility to physically delete historical data which shall be on a user-specified periodic batch basis.

(c) Facility to archive audit logs on a periodic batch basis. The archival period shall be user-specified.

(d) Facility to physically delete revoked accounts which have been inactive for a period defined by authorised users.

4.5. VULNERABILITY ASSESSMENT AND PENETRATION TEST

4.5.1. The Tenderer shall perform vulnerability assessment and penetration test (VAPT) 'Grey Box Testing' on the proposed system. The VAPT shall be conducted by a third-party company and the pen tester must be CREST certified. The Tenderer shall provide the CV of the pen tester and his/her CREST certification.

4.5.2. The Tenderer shall conduct vulnerability scanning quarterly and penetration test yearly.

4.5.3. The Tenderer shall provide the VAPT report to e2i and rectify the vulnerabilities, weaknesses, or errors with no additional cost to e2i.

4.5.4. The Tenderer shall conduct and / or after major updates e.g. Platform versioning, Operating System, Web Servers, Applications) VAPT to ensure no new vulnerabilities are introduced.

4.5.5. Where technical vulnerability assessment and penetration testing cannot be implemented due to limiting conditions such as in Software-as-a-Service model, vulnerability assessment

and penetration testing reports from the service provider are admissible. Outcomes of these reports shall be included into the Technical Risk Assessment.

4.6. DATA RETENTION AND ARCHIVAL

4.6.1. The System shall retain operational data (active applications, ongoing projects, recent claims, current fund structures) in online storage for periods defined by e2i.

4.6.2. The System shall archive historical data (completed projects, closed applications, old audit logs, obsolete fund structures) to a separate archival storage tier after defined retention periods, while maintaining accessibility for reporting, audit, and compliance purposes.

4.6.3. The System shall retain audit trail data for periods defined by e2i in compliance with audit, regulatory, and legal requirements.

4.6.4. The System shall retain financial transaction records (disbursements, recoveries, POs, invoices) for periods defined by e2i in compliance with accounting standards, tax regulations, and audit requirements.

4.6.5. The System shall support data export from archival storage in structured formats (CSV, JSON, XML, database dump, or other agreed formats) for audit, legal discovery, historical analysis, or migration purposes.

4.6.6. All documents attached to the operational data, historical data, financial transactions should be exportable from the System in their original format (Word, Excel, PDF or other document formats used in the System)

4.6.7. The System shall implement secure data destruction procedures for data beyond retention periods, ensuring complete and irreversible deletion in compliance with data protection regulations and organisational policies.

5. DATA CONVERSION

5.1. The Tenderer shall propose an overall data conversion strategy. It shall incorporate details of data to be converted to ensure that the System, when implemented, shall contain correct and consistent data.

5.2. The Tenderer shall estimate the effort required from users, the estimated transition period required in purifying the data and performing the migration, and the manner to manage the

transition period shall also be specified. The Tenderer shall provide a Data Conversion Plan together with the Design Specifications.

5.3. The Tenderer shall ensure that there is minimal impact to the users during conversion process. The conversion shall not cause any system unavailability to the users.

5.4. Converted data shall be consistent and clean. The System shall provide full details of records converted and checks (e.g. number of entities/records converted) to verify the accuracy of the conversion and to ensure database integrity.

5.5. If there are data to be corrected as a result of the conversion, the Tenderer shall provide the means to correct these data. Access to such programs must be controlled and listings/reports on the correction shall be provided.

5.6. The System shall provide means to verify the accuracy of data conversion and data loading. These shall be generic and shall be able to provide details of the data before and after conversion.

5.7. The Tenderer shall propose a Data Conversion Plan detailing the strategy, what data and how the data would be converted to ensure that the System, when first implemented, shall contain correct and consistent data. The estimated effort required from users, the estimated transition period required cleansing the data and performing the migration, and the manner to manage the transition period shall also be specified. The Tenderer shall coordinate and advise e2i on all necessary activities.

5.8. The Tenderer shall ensure that its proposed strategy for data conversion does not jeopardise and has minimal disruption in their use of existing systems.

5.9. The Tenderer shall be responsible for the extraction of the data from the existing systems and coordinating with the relevant e2i representatives on any possible data verification required before the transformation (e.g. mapping, cleansing) of the data.

5.10. The Tenderer shall be responsible for coordinating with the relevant e2i representatives to identify the transformation (e.g. mapping, cleansing) of the data from existing systems to the data and formats required in the new system.

5.11. The Tenderer shall provide the data transformation facilities or programs and set up the transformation rules for the data conversion. As far as possible, all required data shall be converted from the existing computerise systems.

5.12. The Tenderer shall propose in its Data Conversion Plan how to capture additional data items, relating to the same periods as data which are capture in existing Systems, required by e2i for the System.

5.13. The Tenderer shall then supply the necessary data capturing mechanisms (e.g. spreadsheets, data entry applications) for the capturing of such data and coordinate and advise all such activities. All necessary validation checks to ensure that the data loaded into the System are clean and consistent, shall be built in the data capturing mechanisms or data loading programs.

5.14. The Tenderer shall be responsible for and shall bear the cost of rectifying the data in the System or data in the existing system if any inaccurate data arise due to any negligence or error on the part of the Tenderer.

5.15. If the proposed System requires data of periods beyond what have been captured by the existing systems, the Tenderer shall highlight this in its proposal.

5.16. If any data required by the new System is unavailable in the existing System, the Tenderer shall be responsible for the following:

(a) Coordinating the collection of these data.

(b) Ensure that the data required are fully captured and verified for consistency prior to loading into the System; and

(c) Successfully loading the data into the new System.

5.17. The Tenderer shall ensure that the backup process/operation is not run during the Support Hours in any month and shall not affect the performance of the System.

5.18. The Tenderer shall provide facilities to verify the accuracy of the conversion.

5.19. The facilities shall be generic and shall be able to provide details of the data before and after conversion.

6. SYSTEM ACCEPTANCE

6.1. USER ACCEPTANCE TEST PLAN

6.1.1. The Tenderer shall submit a comprehensive user acceptance test plan for user acceptance testing (UAT) of the System or for any other major enhancement, work order and software patch.

6.1.2. The actual scope of testing, the user acceptance criteria and schedule of testing must be submitted by the Tenderer at least two (2) weeks (unless otherwise mutually agreed date) prior to the actual conduct of the test.

6.2. DELAY IN USER ACCEPTANCE TESTING

6.2.1. If in the opinion of the e2i, the UATs are being unreasonably delayed, the e2i may by notice in writing require the Tenderer to conduct the tests within five (5) working days from the receipt of the notice. The Tenderer shall conduct the tests on such date(s) within the said five (5) working days and inform the e2i of the scheduled date(s).

6.2.2. If the Tenderer fails to conduct such tests within the time, the e2i may itself proceed to conduct the said tests. All UATs so conducted by the e2i shall be at the risk and expense of the Tenderer.

6.3. SYSTEM TESTING

6.3.1. The Tenderer shall ensure that comprehensive and relevant tests (unit, integration and system testing) are conducted as dictated by the System requirements. Test plan and test records shall be provided to the e2i for review at least two (2) weeks prior to the User Acceptance Testing (UAT), failing which the e2i reserves the right to hold back the UAT until the test plan and records are produced.

6.3.2. The Tenderer shall propose the testing methodology to be used in the development of the System in the tender proposal. The methodology or set of methodologies shall be reviewed and endorsed by the e2i prior to the development phase of the System.

6.3.3. The Tenderer shall ensure that its development team implements the error checks workflow correctly and consistently, with prior approval obtained from the e2i's Representative which shall validate that these are in accordance to best practice in this area.

6.3.4. The Tenderer shall generate and simulate sufficient test data with the requisite level of complexity/details, and of acceptable quality and quantity by the e2i, to support the required testings and UATs at no additional cost to the e2i.

6.3.5. The Tenderer shall perform end-to-end testing of the System and ensure the System is working correctly in accordance to the requirements specified by the users.

6.3.6. The Tenderer shall perform functional testing on the batch processing to ensure that all batch jobs are completed successfully within the 4 hours of batch window.

6.3.7. The Tenderer shall submit system test report three (3) weeks prior to the commencement of UAT. The Tenderer shall provide supporting evidence on code review, test coverage, tools used, test plan and test cases.

6.4. PERFORMANCE TESTING

6.4.1. The Tenderer shall advise on all matters relating to the installation, configuration, operation and performance tuning of the System.

6.4.2. The Tenderer is required to perform performance load and stress test before System commissioning to meet performance requirements of the System.

6.4.3. The Tenderer must submit the performance load and stress test report two (2) days after the test is carried out to substantiate the ability of the System to meet the performance criteria and manage the number of users logging on at the same time.

6.4.4. In the event that the System utilizes more than the stated System resources, the Tenderer is required to analyse the cause, advice and fine-tune the System at no cost to e2i.

6.5. USER ACCEPTANCE TESTS

6.5.1. If the UAT were to be conducted in the e2i's existing UAT facility, the Tenderer shall work with the e2i appointed FM Team to set up the entire UAT environment at least one (1) week prior to the commencement of each UAT, and ensure it is complete and in fully functional condition for the UAT.

6.5.2. If the UAT were to be conducted outside e2i, the Tenderer shall be responsible for setting up the entire UAT environment at no additional cost to the e2i.

6.5.3. The Tenderer shall be responsible for the preparation and refresh of base set of all needful test data required for the independent testings and UAT which include end to end flow testings at no additional cost to the e2i.

6.5.4. Where applicable, the Tenderer shall prepare a plan for setting up the UAT environment and the configuration of the environment, including the hardware, system software, which is required to implement the application system. The Plan shall be supplied for the e2i's approval at least three (3) weeks before the commencement of the UAT.

6.5.5. The Tenderer shall provide training for the e2i for those who are identified to conduct the UAT, in order to guide the personnel on how to conduct the tests, including all test scenarios and pass/ fail criteria for the test items, as well as interpretation of the test results.

6.5.6. The Training shall cover the following: -

(a) Guidance on the scope of the tests and test scenarios which shall be prepared by the Tenderer, and interpretation of test results, and logging of actual test observations/results for the application system. This shall include assessment of the test results and assignment of Pass/Fail criteria for each test item/scenario, proper and consistent documentation of test results and observations; and

(b) Use of the System.

6.5.7. The Training shall be conducted at least one (1) week before the UAT. The Tenderer shall note that the Training shall be conducted for major enhancements and work orders only.

6.5.8. The Tenderer shall provide on-site full-time qualified and competent personnel with relevant UAT hands-on experience to follow through all the testing required and to perform the necessary documentation of test results, particularly bugs detected, for discussion and resolution subject to agreement with the e2i. The Tenderer shall provide advice and assistance to the e2i on the carrying out of the UAT, and solve any problems encountered during the UAT period promptly so that the UAT can be completed as planned, including clear/ unambiguous criteria for abandoning an UAT.

6.5.9. The Tenderer is responsible for documenting all UAT defect logs and consolidating the defects into a summary with the required details on problem cause, propose resolution actions and timelines for agreement by the e2i, and thereafter, to facilitate monitoring of defects fixing, re-testing and proper closure within the agreed timelines.

6.5.10. The Tenderer shall update the consolidated defect log daily and submit the updated consolidated defect log to the e2i by noon on the following day.

7. SYSTEM PERFORMANCE, AVAILABILITY AND RELIABILITY

7.1. SYSTEM PERFORMANCE AND RESILIENCY

7.1.1. The online response time shall be measured as the elapsed time between the moment a user initiates a computer process by pressing a key or clicking a mouse or touching the screen or other input device and the moment the last display of the first screen of the resulting computer-generated output is seen on the screen of the computer. A computer

process can be a query or an update to a database, a request of an electronic document or any other logical unit of business transactions that involve interactive responses.

7.1.2. The System shall support online transactions, scheduled batch jobs as well as ad hoc batch jobs / reports submitted by the users.

7.1.3. The System shall meet the Response Times as stated below. In the event that the Response Time cannot meet due to whatever reasons, the Tenderer shall carry out all necessary remedial actions and remedial services at no extra cost to e2i. In the event that the Tenderer diagnosed and show concrete evidence that the problem is due to a component managed by e2i, The Tenderer shall be required to propose the necessary recommendation to e2i to resolve the problem.

System Response Time

Function	System Response Time
On-line update	Shall not exceed five (5) seconds
On-line enquiry/screening	Shall not exceed three (3) seconds
Reporting	Shall not exceed five (5) minutes for 90% of the time; and Shall not exceed fifteen (15) minutes for the remaining 10% of the time
Batch processes	To be run after the Midnight and completed by 6:00am.

7.1.4. The Tenderer shall monitor the performance on an on-going basis and review the existing network infrastructure and satisfy itself that the required System Response Time could be met as data grows.

7.1.5. The Tenderer shall highlight to e2i, in detail, all necessary actions/upgrades required for the existing network infrastructure, if according to its expert opinion, the existing network infrastructure could not satisfy the performance requirements. Failing which, the Tenderer shall bear all required to achieve the required System Response Time.

7.1.6. The Tenderer shall describe the methods and calculations used for computing the expected online response times subject to the above conditions.

7.1.7. The Tenderer shall fine-tune the System, when necessary, as requested by e2i to ensure the System meets the System Response Time as specified.

7.2. SYSTEM COMMISSION

7.2.1. The System shall be commissioned upon the successful implementation in the production environment including the following pre-implementation activities for the System delivery:

(a) User Acceptance Test is completed successfully

(b) Performance Test is completed successfully

(c) Training for users of the System is completed

(d) VAPT is completed and risk(s) remediated, if any, successfully

7.2.2. If there is a failure to meet the completion of either Delivery Phase, the Go-Live Date or Completion Date, and such delay is caused by the acts or omissions of the Tenderer or any of its third-party suppliers:

(a) the Tenderer shall pay to e2i for each day after the scheduled Delivery Phase Date until the date when the Tenderer completes the relevant Delivery Phase the sum specified in Clause 9.3.14 as liquidated damages, and the Tenderer agrees that this sum is proportionate when considering e2i's legitimate interest to avoid any delay in the completion of the Delivery Phase;

(b) the Tenderer shall pay to e2i each day after the scheduled Go-Live Date until the date when the Tenderer will complete the design, build and delivery to the Site of the System the sum specified in Clause 9.3.14 as liquidated damages, and the Tenderer agrees that this sum is proportionate when considering e2i's legitimate interest to avoid any delay in the design, build and delivery to the Site of the System;

(c) the Tenderer shall pay to e2i for each day after the scheduled Completion Date until the date when the System is Ready for Service the sum specified in Clause 9.3.14. as liquidated damages, and the Contractor agrees that this sum is proportionate when considering e2i's legitimate interest to avoid any delay in provision of the System to be Ready for Service;

(d) e2i may engage another contractor to provide the System and/or the Services, and any resulting increased costs incurred by e2i will be chargeable as a debt due from the Tenderer to e2i; and/or

(e) unless otherwise agreed between the Parties in writing, If the Tenderer fails to meet any Delivery Phase Date, the Go-Live Date or make the System Ready for Service by more than twelve (12) weeks after the scheduled Delivery Phase Date, Go-Live Date or Completion Date respectively, without prejudice to any other rights or remedies, e2i may immediately terminate the Contract by giving written notice to the Tenderer. Parties acknowledge and agree that a failure of the

Tenderer to meet the scheduled Delivery Phase Date, Go-Live Date or Completion Date shall constitute a material breach of the Contract.

7.3. PERFORMANCE GUARRANTEE PERIOD

7.3.1. Performance Guarantee Period (PGP) shall commence after the System Commissioning Date.

7.3.2. The Performance Guarantee Period of six (6) calendar months.

7.3.3. The Tenderer shall provide the necessary system performance tools during the PGP to e2i to monitor the System's response time, resource utilization, and network traffic. The provision of such tools shall be at no additional costs to e2i.

7.3.4. During the Performance Guarantee Period, the Tenderer may be required to service change requests that cannot be delayed during this period.

7.3.5. System Performance requirements stated in Clause 7.1.3 shall apply during the Performance Guarantee Period.

7.3.6. In the event that the System fails to meet the System Performance Requirements, the PGP shall be extended until the System Performance Requirements are met.

7.3.7. The Tenderer shall, at his or her own costs restore the System to an operable state when the system downtime is attributable to errors or faults in the Tenderer's customization / development effort for the System.

7.3.8. The Tenderer shall maintain the same man-day rate for servicing change requests during the performance guarantee period. For each change request, the Tenderer shall advise e2i

on the cost and impact of changes that affect the system performance. The implementation of change request(s) shall be subjected to e2i's approval.

7.3.9. The end of the Performance Guarantee Period shall be the System Acceptance Date for the system.

7.4. SYSTEM WARRANTY

7.4.1. The System Warranty shall commence after System Acceptance.

7.4.2. The Tenderer shall provide a warranty period of twelve (12) months for all the services delivered.

7.4.3. The Tenderer shall, at his or her own costs, restore the System to an operable state when the system downtime is attributable to errors or faults in the Tenderer's customization / development effort for the System.

7.4.4. The Tenderer may require providing support services to the System during the System Warranty Period to ensure the System performs as expected.

7.4.5. During the Warranty Period, the Tenderer may be required to service change requests that cannot be delayed during this period.

7.4.6. The Tenderer shall maintain the same man-day rate for servicing change requests during the warranty period. For each change request, the Tenderer shall advise e2i on the cost and impact of changes that affect the system performance. The implementation of change request(s) shall be subjected to the e2i's approval.

7.5. SYSTEM AVAILABILITY

7.5.1. The Tenderer shall maintain the System Availability of at least ninety-nine-point five percent (99.5%) per month.

7.5.2. The System Availability shall be determined according to the following formula:

(a) "System availability = [Scheduled Operation Time - System Downtime] / [Scheduled Operation Time] x 100%.

(b) "System Downtime" means the accumulated time during which the System is not performing in accordance with the Standard of Performance due to product failure measured from the time the Supplier is informed by phone of the product failure to the time when the System is returned to proper operation.

SUPPORT HOURS & OPERATING HOURS

7.5.3. The Support Hours of the System are:

Monday - Friday: 9:00am - 6:30pm

Saturday: 9:00am - 1:00pm (Exclude Sundays & Public Holidays)

7.5.4. The Operating Hours of the System is TWENTY-FOUR (24) hours every day, including Sunday and Public Holidays.

7.5.5. The Tenderer's key personnel shall be contactable at all times via mobile phone. The support staff may be activated after office hour to resolve critical problems.

7.5.6. Upon notification of the problem, the Tenderer's personnel must respond within the required time specified in Clause 9.3.2 during the support hours of the system.

8. SYSTEM SECURITY AND AUDIT

8.1. GENERAL REQUIREMENTS

8.1.1. The Tenderer shall comply with the IT Security Standards for Application and Infrastructure and any other related standards/procedures by the e2i's Representative.

(A copy of the relevant IT Security Standards can be requested for the purpose of this tender. The Tenderer shall sign an undertaking upon receipt of the above document declaring that he is only using it for the purpose of the tender and shall be returning the document after the tender. No copy of the document is to be duplicated without prior approval from e2i.)

8.1.2. The Tenderer shall comply with IT Security Policies and any other related policies, standards, procedures and regulations provided by e2i.The security audit requirement details shall be made available only to The Tenderer. The business users will provide a set of audit requirement for sensitive transactions to be audited.

8.1.3. The System shall include audit trail and audit log capabilities for system and database operational activities. The audit trails shall not affect the systems performance significantly where it impacts users' experience.

8.1.4. The Tenderer shall ensure provision of necessary security features to guard the System and interface with external systems against all malicious intents such as unauthorised access, intrusion, loss of information, software error and vulnerability to virus attacks.

8.1.5. The Tenderer shall ensure that the System has the appropriate SSL version to be used as the web access method.

8.1.6. Transmission of ID and password and any other information deemed as sensitive shall be encrypted.

8.1.7. Timeout and logout features shall be set for non-active session web and client server access. The timeout period feature should be configurable. As far as possible, the System shall warn the users of impending timeouts.

8.1.8. The System developed shall not contain any hidden functionalities which e2i is not aware of and e2i has the rights to perform security review to ensure the compliance of this clause and all the security requirements are met.

8.1.9. The Tenderer shall provide a Security Operation Center (SOC) to monitor and analyze the network, firewalls and systems traffic, logs and configurations to identify potential security risk, and shall provide detailed report to e2i and work with the Infrastructure Management Team to mitigate or remove the risk. The Tenderer shall describe in detail, any other security and control features that support intent of this clause.

8.1.10. The System shall not send unprotected or plain text password emails to users when user accounts are created or when users request a password reset.

8.1.11. The Tenderer shall ensure that all system resources or sessions can only be accessed via valid authenticated users.

8.1.12. The System shall not allow auto-completion attributes in any system form, especially input elements that contain passwords or other sensitive information.

8.1.13. The System must terminate the user session on the server/application when a user logs out of the system.

8.1.14. The System shall have proper cache controls.

8.1.15. The System shall disable any weak SSL cipher suites on all SSL/TLS based services.

8.1.16. The Tenderer shall implement CAPTCHA controls on logins or those which may initialize additional processes to mitigate against an attacker submitting them in an automated manner.

8.1.17. The System must support the latest version of TLS.

8.1.18. The System shall have the ability to enable encryption of user identity and information at login.

8.1.19. The System shall have the ability to mask sensitive information within the system and only accessible by authorized users.

8.1.20. The System shall ensure PDPA compliance, and where possible, GDPR compliance.

8.1.21. The Tenderer shall perform security hardening for the System to minimise attack surface and to reduce the exposure to security risks. Security hardening includes:

(a) Disabling all unused ports;

(b) Uninstall or disabling non-essential and unused OS services / packages;

(c) Restrict administrative rights of users;

(d) Network whitelisting approach for all implemented network equipment and security devices;

(e) Application whitelisting to prevent unauthorised software execution and/or installation;

(f) Disabling of PowerShell;

(g) Replacement of all default passwords and configurations; and

(h) Controls on the use of removable media and portable equipment in the System's environment.

8.1.22. The Tenderer shall ensure all security hardening practices are to be documented and submitted to e2i as part of documentation requirements.

8.1.23. The Tenderer shall ensure that the submitted document is updated and current as reflected on the practices.

8.2. AUTHENTICATION AND ACCESS CONTROL

8.2.1. The purpose of the authentication service is to check and validate the identity of a user. Other security services, such as access control or audit, are dependent on the authentication service to ensure that the identification of a user is correctly established. The authentication service must be strong and robust.

8.2.2. The System shall cater for multiple types of login method (eg. Singpass, mobile number, email, other request login platform) for the different groups of user logins.

8.2.3. The System shall be ready to allow integration with third party authentication tools / Identity Management tools (e.g. Okta).

8.2.4. The System shall have the ability to configure Two-Factor Authentication (2FA) or multi-factor authentication for all user accounts.

8.2.5. e2i shall reserve the rights to choose the type and form factor of the 2FA/MFA solution.

8.2.6. The 2FA/MFA authentication method shall be minimally:

(a) Mobile application digital token authentication with Time-Based One Time Password (TOTP) (Apple IOS or Android OS)

(b) Short Message Service (SMS) gateway through HTTP(S) or SMTP protocol to generate and verify SMS One-Time Password (OTP).

(c) Voice call back to registered Account User telephone number

8.2.7. Once a user is successfully authenticated, he shall be able to access all authorised services provided by the Systems without the need for further authentication.

8.2.8. An authenticated user shall not be allowed to access information that he/she has no rights to via any means or through the exploitation of system weakness/vulnerability.

8.2.9. The System shall log out a user if there is no activity for a period that is to be defined by the System Administrator. Upon session expired or system logoff, whenever user click on the "back" button, they shall be prompted for re- authentication.

8.2.10. e2i shall have the overall administrative access to the System but not limited to the following (Infrastructure, Databases, Applications)

8.2.11. Segregation of roles shall be clearly defined and documented for Privileged Users.

8.2.12. Privileged Users refer to users such as system administrator of operating system, database administrator, and user account operator.

8.2.13. Privileged access shall be given to user on a "need-to-use" basis.

8.2.14. Sufficiently strong access controls shall be used to prevent unauthorised Privileged Users from accessing important system resources, including the use of tamper-evident in the audit trails.

8.2.15. The System shall comply with e2i's Password Policy and e2i's User Account and Access Management Policy. The policy details shall be made available only to The Tenderer.

8.3. SECURITY MANAGEMENT AND ADMINISTRATION

8.3.1. The Tenderer shall establish procedures for the application of new system accounts and the termination of obsolete accounts on the proposed system servers according to e2i's User Account and Access Management Policy.

8.3.2. The Tenderer shall manage the role creation and maintenance of the proposed System.

8.3.3. The System shall have the capabilities to enforce access control where users can be grouped into roles having specific functions and access rights.

8.3.4. The Tenderer shall work with systems owners, auditors and security function to ensure proper segregation of duties between the different roles of the systems.

8.3.5. The proposed System shall provide security controls/measures to ensure that each of the following required security requirements are met:

(a) Confidentiality: Ensure that data/information is accessible only to those authorised personnel and it is used solely for the purposes of performing the Subscription Contract unless e2i gives the Tenderer written authorisation for the data/information to be used for other purposes

(b) Integrity: Ensure that data is unchanged from its source and has not been accidentally or maliciously modified (e.g., SQL injection, cross-site scripting), altered or destroyed without proper authorization to safeguard the accuracy and completeness of data

(c) Accountability Ensure that actions carried out at various stages are properly tracked and can be traceable to the user who performed the action

(d) Authorisation: Ensure that the granting of rights is based on access privileges (e.g., user roles)

8.3.6. The proposed System shall ensure that the design and implementation of the solution is not affected by vulnerabilities listed under Top 10 OWASP (Open Web Application Security Project).

8.3.7. The Tenderer shall ensure that the customised codes are secured and not affected by known security vulnerabilities.

8.3.8. The Tenderer shall use the industry recognised or OWASP's recommended static code analysis tool to perform and carry out code reviews upon

(a) Completion of development/coding

(b) Major updates to the codes

(c) As and when requested by e2i

8.3.9. The Tenderer shall implement single user logon session if the System is able to support this feature.

8.3.10. All sensitive and personal data collected shall be encrypted and compliant with the Singapore Personal Data Protection Act (PDPA).

8.3.11. All sensitive and personal data collected shall be hosted in Singapore. In the event where there is deviation, it is the responsibility of the Tenderer to seek e2i's approval for data hosting in other countries and to provide details on how data sovereignty will be ensured.

8.3.12. It is recommended for The Tenderer to have the recognised certifications of high standards of practices such as IMDA's Data Protection Trustmark (DPTM) or ISO's Information Security Information System (ISO 27001/27002).

8.3.13. The proposed System must employ a firewall that does not permit application from sending traffic with a source IP or MAC address other than its own.

8.3.14. The proposed Systsem should provide the ability to filter requests by IP, enabling e2i to limit traffic to trusted networks. The service should have basic Data Loss Prevention mechanisms, such as traffic reporting and alerting of traffics above a set threshold or a provider-determined baseline.

8.4. INFORMATION INTEGRITY

8.4.1. The Tenderer shall embed data integrity features to protect data from being altered or deleted without proper authorisation.

8.4.2. The Tenderer shall ensure that access granted to any data and/or resources shall be approved by system owner or data custodian and filed.

8.5. SYSTEM AUDIT

8.5.1. The Tenderer shall allow the appointed Tenderer by e2i to conduct periodic audits on the systems.

8.5.2. The Tenderer shall provide all support necessary for the conduct of the audits at no additional cost to the Customer.

8.5.3. The Tenderer shall ensure that the System is able to capture audit trails of the following:

(a) Selected "create", "update" and "delete" transactions performed, for e.g. transaction that will impact financial data

(b) Network

(c) Operating Systems (OS)

(d) Web & Application Servers

(e) Databases

(f) The information to be logged includes the user identifier such as user id and machine name, the action taken and the date and time stamp of these transactions.

8.5.4. The System shall capture audit information on illegal access of data or to System functions.

8.5.5. The System shall allow only authorised users to view the audit information.

8.5.6. The System shall ensure that these audit trails be protected from being modified including privilege users.

8.5.7. The System shall have the facility to store the audit information online for varying periods depending on the type of audit trails before they are archived to a media proposed by the Tenderer. The media proposed shall be subjected to the approval of e2i. The general guideline would be three (3) months online for database audit trail and three (3) months online for other audit trails.

8.5.8. The System shall provide capabilities to search/query audit logs and generate audit log reports.

8.6. AUDIT

8.6.1. The Contractor shall permit e2i to conduct such audit or other inspection of Services provided to e2i, as e2i deems necessary. Such inspection shall also include the examination of any materials, documents, equipment, premises and facilities relating to the Services provided under this Contract that are within the possession, custody or control of the Contractor. e2i shall inform the Contractor in advance for any inspections and the Contractor shall ensure that such inspections shall not affect the Service Levels. The right of audit may be extended to the Contractor's subcontractors who are involved in the project.

8.6.2. The Contractor shall provide the resources necessary to work with e2i's appointed auditors to assist in the audit and its review at no additional cost to e2i.

8.6.3. The Contractor shall implement the audit recommendations and provide evidence for the audit recommendations carried out, to e2i not later than one (1) calendar month after e2i's approval of the audit report.

8.6.4. The Contractor shall propose follow-up plans to address audit findings, subject to e2i's approval. The proposal shall include a schedule of the closure of audit findings, subject to mutual agreement.

8.6.5. The Contractor shall monitor and ensure that corrective follow-up actions are carried out for the audit findings. The Contractor shall provide evidence, for the corrective follow-up actions carried out, to e2i no later than one (1) calendar month after e2i's approval of the audit report.

8.6.6. The implementation of the audit recommendations and corrections shall be done at no additional cost to e2i if the audit gaps are due to the Contractor's failure to meet the Requirements Specifications.

8.7. SECURITY MEASURES

8.7.1. The System shall be implemented to include the following security measures:

8.7.2. Use of cloud native network firewalls, web application firewalls or equivalent as required by NTUC/e2i policies, guidelines, and conventions.

8.7.3. The system shall be protected by a properly configured Web Application Firewall (WAF) to mitigate common web-based attacks. WAF rules shall be securely configured and optimised to minimise exceptions. Any exceptions shall be limited, justified, documented, and approved through formal risk management and change control processes.

8.7.4. The Contractor shall ensure that all required network connectivity for the system is formally documented, including source and destination details, ports, protocols, and data flow justifications. All firewall rules shall be subject to prior review, risk assessment, and approval through the established change management process. Periodic reviews shall be conducted to validate the continued necessity of such connectivity, and any unused or unnecessary rules shall be promptly removed.

8.7.5. Use of cloud security detection tools or equivalent as required by NTUC/e2i policies, guidelines, and conventions.

8.7.6. Use of cloud native logs or equivalent as required by NTUC/e2i policies, guidelines, and conventions.

8.7.7. Automated notifications when suspicious activities are detected.

8.7.8. Ensure logs are streamed to designated endpoints such as monitoring and security platforms.

8.7.9. Log all access to personal data.

8.7.10. Encrypt data at rest and in transit in accordance with NTUC/e2i policies, guidelines, and conventions.

8.7.11. Put in place access controls following the principle of least privilege and ensure that access is only given to authorised users.

8.7.12. The contractor shall integrate with NTUC/e2i's existing secure file upload mechanisms (if applicable).

8.7.13. The Contractor shall perform quarterly Vulnerability Assessment and annual Penetration Testing (VAPT) on System and fix all necessary issues according to NTUC policies, guidelines, and conventions before going live.

8.7.14. The Contractor shall comply with all of NTUC/e2i's policies and procedures, including the NTUC/e2i IT Policy and Cybersecurity Governance and Escalation Framework.

8.7.15. The Contractor shall utilise NTUC/e2i's existing Privileged Access Management ("PAM") solution currently in place for all relevant activities. The System developed by the Contractor shall be designed and implemented to seamlessly integrate with the existing PAM environment, ensuring secure, interoperable, and policy-compliant access controls in accordance with established PAM processes.

8.7.16. The Contractor shall adhere to recognised cybersecurity standards and frameworks, including but not limited to ISO/IEC 27001, NIST Cybersecurity Framework, or equivalent standards deemed appropriate by NTUC/e2i.

8.7.17. The Contractor shall establish and maintain documented cryptographic key-management procedures covering the generation, storage, distribution, activation, use, rotation, revocation, recovery, backup, archival and secure destruction of cryptographic keys and certificates used by the System.

8.7.18. Cryptographic keys shall be protected against unauthorised disclosure, modification, substitution and destruction throughout their lifecycle and shall be stored only in security mechanisms approved by e2i.

8.7.19. Access to cryptographic keys and key-management functions shall be restricted on a least-privilege basis, subject to appropriate segregation of duties, multi-factor authentication and audit logging.

8.7.20. The Contractor shall define and implement key-rotation and certificate-renewal periods appropriate to the sensitivity and risk of the protected information, and shall rotate or revoke affected keys promptly upon suspected compromise, personnel changes or material changes to the System.

8.7.21. Unless otherwise approved in writing by e2i, the Contractor shall not retain sole and exclusive control of cryptographic keys required for e2i to access, recover, migrate or securely exit the System. Key ownership, custody and access arrangements shall be documented and approved by e2i.

8.7.22. The Contractor shall monitor certificate and key expiry dates and shall complete renewal or replacement sufficiently in advance to prevent service disruption.

8.8. CYBER INCIDENT AND DATA BREACH NOTIFICATION

8.8.1. The Contractor shall notify e2i immediately upon becoming aware of any actual or suspected Cybersecurity Incident affecting, or reasonably likely to affect, the System, the Services, e2i Data, Personal Data, e2i systems or any connection to e2i systems. In any event, the initial notification shall be made no later than two (2) hours after discovery.

8.8.2. For the purposes of this Clause, a "Cybersecurity Incident" includes any actual or suspected unauthorised access, use, disclosure, alteration, loss, destruction or exfiltration of data; compromise of accounts, credentials, systems or networks; malware or ransomware infection; denial-of-service attack; material security-control failure; or other event that may compromise the confidentiality, integrity or availability of the System, the Services or e2i Data.

8.8.3. The initial notification shall include, to the extent known at the time: (a) the date and time of discovery; (b) the nature and scope of the Cybersecurity Incident; (c) the systems, services, data and persons affected or potentially affected; (d) the containment and remediation measures taken or proposed; (e) the known or suspected cause; and (f) the contact particulars of the Contractor's incident coordinator.

8.8.4. The Contractor shall provide e2i with regular written updates at intervals directed by e2i until the Cybersecurity Incident has been contained, remediated and closed. The Contractor shall notify e2i promptly of any material change in the facts, impact, risk assessment or remediation plan.

8.8.5. The Contractor shall, at no additional cost to e2i, take all necessary steps to contain, investigate, remediate and prevent recurrence of the Cybersecurity Incident; preserve relevant logs and evidence; and provide all reasonable assistance required by e2i, its appointed investigators, auditors, regulators and law-enforcement authorities.

8.8.6. The Contractor shall not make any public statement, notify any affected person or regulatory authority, or communicate with the media concerning the Cybersecurity Incident without e2i's prior written approval, unless the Contractor is required to do so by applicable law. Where legally permitted, the Contractor shall consult e2i before making such notification or statement.

8.8.7. The Contractor shall submit a preliminary incident report within one (1) working day after discovery and a detailed root-cause analysis and post-incident report within five (5) working days after containment, or within such other period approved by e2i. The detailed report shall include the root cause, chronology, impact, evidence reviewed, corrective and preventive actions, owners and completion dates.

8.9. SECURE SOFTWARE DEVELOPMENT LIFECYCLE

8.9.1. The Contractor shall establish, document, implement and maintain a Secure Software Development Lifecycle ("Secure SDLC") for the design, development, configuration, integration, testing, deployment and maintenance of the System.

8.9.2. The Secure SDLC shall incorporate security-by-design and privacy-by-design principles and shall include, at a minimum: (a) security requirements definition; (b) threat modelling and security design review; (c) secure coding standards; (d) peer code review; (e) software composition and dependency analysis; (f) static application security testing; (g) dynamic application security testing; (h) vulnerability assessment and penetration testing; and (i) security verification before release to Production.

8.9.3. The Contractor shall ensure that security requirements and security acceptance criteria are traceable through the requirements, design, development, testing and release stages.

8.9.4. The Contractor shall use suitably configured and maintained security testing tools and shall review, triage and remediate findings in accordance with the vulnerability remediation requirements in this Annex.

8.9.5. The Contractor shall maintain evidence of Secure SDLC activities, including threat models, design-review records, code-review records, test results, vulnerability findings, remediation records and release approvals, and shall provide such evidence to e2i upon request.

8.9.6. No software release shall be deployed to Production unless the Contractor has completed the required security activities and obtained the approvals required under the agreed release and change-management process.

8.9.7. The Contractor shall ensure that all personnel involved in the design, development, testing and maintenance of the System receive appropriate secure-development training relevant to their roles and responsibilities.

9. CHANGE AND PROBLEM MANAGEMENT

9.1. INTRODUCTION

9.1.1. The aim of change management is to ensure that all proposals for changes to the proposed System are properly evaluated in terms of their costs and benefits, and their priorities. Such changes include alterations to the System administration and operational procedures. It will also monitor the progress of change requests

9.1.2. The aim of problem management is to ensure that all problems are attended to as quickly as possible so that disruption to the operation is minimized.

9.1.3. Clause 12.2 of the Tender Document shall be applicable during the whole development cycle, Performance Guarantee Period, System Warranty Period and subsequent maintenance period, if awarded.

9.2. CHANGE MANAGEMENT

9.2.1. The Tenderer shall state explicitly the specific costs associated with Change Management in the Tender Proposal.

9.2.2. The Tenderer shall also propose the man-day rate and man-days required for change requests according to the Clause 16.2. e2i may exercise the right to engage such services from the Tenderer on the basis of man-day rates and man-days required.

9.2.3. Should e2i exercise the option to award CR, the Tenderer shall undertake the Work Order.

9.2.4. The Tenderer shall provide a schedule for the Change Management activities.

9.2.5. The Tenderer shall also show how this schedule and activities ties in with the various phases of the project e.g. requirements gathering, System development, installation, testing schedule, etc.

9.2.6. The Tenderer shall develop a detailed Change Management Plan to enable the acceptance of the System by all stakeholders. This is to ensure a smooth implementation of the System and minimal impact to e2i's business operations.

9.2.7. The Tenderer shall assist e2i to manage expectations of stakeholders.

9.2.8. The Change Management Plan shall at least:

(a) Assess the change impacts of the system re-implementation to mitigate change risks and help e2i to realize the benefits of the re-implementation.

(b) Document the change management process decisions, activities and tasks required for the project

(c) Develop and execute communications plan to e2i process owners and users

(d) Assess training needs and develop training plan

(e) Propose an approach to introduce the System functionalities to the different groups of users not involved in the project team

(f) Document the change management strategy and activities and other relevant information so that they are well understood by all relevant parties.

9.2.9. The Tenderer shall be responsible for the execution of the change management and communication plan.

9.2.10. The Tenderer shall propose the format for the CR Proposal which will detail the impact of changes to the System. The format of the CR Proposal shall be approved by e2i.

9.2.11. The Tenderer shall ensure that all approved CRs are completed and implemented based mutual agreement between the Tenderer and e2i.

9.2.12. Customisations and enhancements to the System shall be subjected to functionality and performance tests.

9.2.13. Notwithstanding approval given by e2i to any of the Tenderer's proposal, design and specifications, the Tenderer shall remain sole responsible for the completeness and adequacy of the design, performance and specifications within the scope.

9.2.14. The Tenderer shall ensure that the proposed customisations and enhancements can be fully integrated, function properly and efficiently with the existing operational modules, without compromising any feature of the proposed solution and shall not cause any degradation to the existing operational modules.

9.2.15. The Tenderer shall be responsible for the smooth integration of the customisations to the existing System. The Tenderer shall be required to troubleshoot any problems and advise e2i accordingly.

9.3. PROBLEM MANANGEMENT

9.3.1. The Tenderer shall follow the Problem Management Procedure endorsed by the e2i.

9.3.2. Unless otherwise specified by e2i in writing, the Tenderer shall provide the following default levels of Services in respect of response and resolution time for problem resolution corresponding to the following classifications:

(a) Service Level Definition

Incident Severity Classification	**Response Time**	**Resolution Time**
Severity Level 1	Within **15 minutes**	Within **2 hours**
Severity Level 2	Within **15 minutes**	Within **8 hours**
Severity Level 3	Within **60 minutes**	Within **4 Business Days**

(b) Incident Severity Classification = Incident Operation Impact x Urgency Of Incident

Incident Severity Matrix		**Incident Operation Impact**			
		Widespread	**Significant**	**Moderate**	**Minor**
Urgency of Incident	High	1 – High	1 – High	1 – High	1 - High
	Medium	1 – High	2 – Medium	2 – Medium	3 - Low
	Low	2 - Medium	2 – Medium	3 - Low	3 - Low

(c) Incident Operation Impact is the measure of impact on operation and is equal to the extent to which an incident leads to degradation of agreed service

Incident Operation Impact	Description	Examples (Not limited to the following)
Widespread	Service unavailable to all users and/or touch points.	1) Failure of Servers 2) Unexpected application and/or database failure 3) Failure of Power where all equipment are hosted.
Significant	Service unavailable to majority of users and/or touch points OR Degradation of service to all	1) Failure of server or equipment with many connected users and/or touch points. ie failure of cloud servers 2) All users and/or touch points users and/or touch points encountered system latency issues (or performance degradation).
Moderate	Service unavailable to minority of users and/or touch points OR Degradation of service to majority of users and/or touch points	1) Failure of server or equipment with many connected users and/or touch points. ie failure of cluster of servers specific to a small group of users 2) Selected users and/or touch points encountered system

		latency issues (or performance degradation).
Minor	Service unavailable to one user and/or touch point OR Degradation of service to minority of users and/or touch points.	1) A few users and/or touch points encountered system latency issues (or performance degradation). 2) Failure of hardware itself or the underlying client OS or software.

(d) Urgency of Incident is a measure of how long System can be down until the incident has a significant impact to the operation. It is equal to the amount of internal and external resources required to stabilize the system.

Urgency of Incident	**Description**	**Examples (Not limited to the following)**
1 - High	Must be resolved immediately AND Correction / workaround resolution available.	1) e2i users are disrupted and unable to perform business operation. 2) Malfunction of application related functions. 3) Failure of application or backend servers that affect operational transaction.

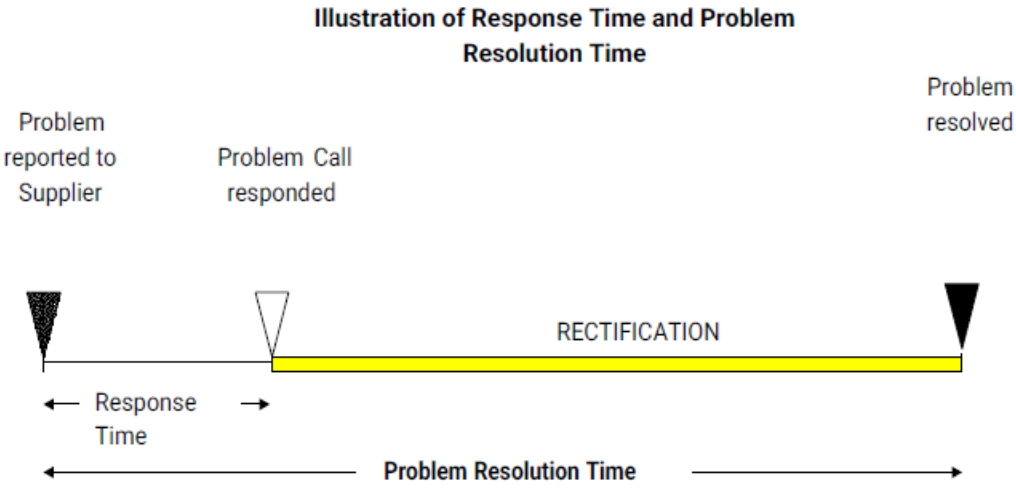
2 - Medium	Needs immediate attention AND Can be resolved at a slightly later time AND Correction / workaround resolution available.	1) Failure of a particular process or system for which there are existing alternatives to bypass the problems.
3 - Low	Can be resolved at a later time AND Corrective and Preventive Action / permanent resolution available	1) Failure of a particular process or system but has minimal or no impact to e2i's ability to perform business operation.

9.3.3. Severity levels are priority levels assigned to the problem based on urgency, number of users affected, type and extent of service disrupted and availability of a workaround or fallback. When a problem is communicated to The Tenderer, e2i will assign the severity level of the problem definition. e2i reserves the right to re-classify the severity levels if the needs arise.

9.3.4. The "Response Time" shall begin from the time or date the problem is communicated to The Tenderer's single point of contact, regardless of whether the single point of contact acknowledges receipt of the message. The message may be communicated by any of the e2i's Helpdesks, the e2i's Representative responsible for the system concerned, or any e2i user through telephone, fax or electronic mail. The "Response Time" ends when a response is provided by The Tenderer for the problem via telephone or electronic mail to the person who reports the problem. (Refer to illustration below).

9.3.5. The "Problem Resolution Time" shall begin upon communication of the problem to The Tenderer's single point of contact, regardless of whether the single point of contact acknowledges receipt of the message. The "Problem Resolution Time" ends when the

problem is resolved, and the defect is restored to a satisfactory working condition (Refer to illustration below).



9.3.6. The Tenderer shall perform a thorough analysis of the problem, which includes identification of the cause of problem, the systems affected, data or any loss suffered and the recommended solution.

9.3.7. For Severity 1 problems, The Tenderer shall provide in writing a preliminary report to explain the incident the following working day. Subsequently The Tenderer shall provide a post incident review report to explain in detail the cause of the incident, the corrective actions taken and the solutions to prevent the incident from recurring, within five (5) working days after the incident has been rectified.

9.3.8. The Tenderer shall provide a mechanism and substantiate to the e2i that Service Levels are met. There must be proper acknowledgement and monitoring of all reported defects and problems by The Tenderer. The Tenderer shall be responsible to ensure that the e2i's Representative is kept updated on the latest status of the reported defects or problems without being prompted. The frequency of status reporting required is shown in the tables in Clause 9.3.2.

9.3.9. The Tenderer shall work with all parties designated by the e2i and take whatever actions to resolve all problems.

9.3.10. In the event of any dispute on the cause of the problem, The Tenderer shall demonstrate and prove services rendered within the scope of this Contract are not the cause of the problem. The Tenderer shall continue to work with the relevant parties to resolve the problem.

9.3.11. The Tenderer shall schedule problem reviews to track unresolved problems and provide rectification effort to prevent problem from recurring. The e2i shall specify frequency of such reviews.

9.3.12. There shall be monthly problem reviews to track unresolved problems and provide rectification efforts to prevent the problem from recurring.

9.3.13. Essentially, for all problems affecting the functioning of the System, The Tenderer shall own the problem and track it from initiation to closure. For this, The Tenderer shall proactively liaise and manage the other Service Providers (i.e. the Data Centre Service Provider, the Facility Management Service Provider, the Managed Network Provider, the System Security Service Provider, and the System Monitoring Service Provider) until the closure of the problem.

9.3.14. In the event The Tenderer is unable to meet the service level as specified, e2i may impose liquidated damages at the rate of as follows in the following Table below (based on more than 1 million contract price).

S/No	**Description of Requirements**	**Source of Requirements**	**Liquidated Damages for failing to meet Requirements (S$)**
1	Failure to comply with any of the Particular Requirements / Specifications	Provisions of the Contract	S$1,000 per occurrence
2	Failure to: (i) complete a Delivery Phase by the respective Delivery Phase Date; (ii) complete the System by the Go-Live Date;	Provisions of the Contract	S$1,000 per day, for every day of delay (including Sundays and Public Holidays)

	(iii) provide the System Ready for Service by the Completion Date; (iv) fulfill the Delivery Date; and/or (v) provide any Services by the dates or within the periods stipulated in this Contract.		
3	Failure to meet the Recovery Time Objective (RTO) set out in Contract* ** Should the issue be caused by third party other than the Contractor, a review by e2i together with the Tenderer will be conducted to ascertain if the issue could have been prevented with the better design of architecture.*	System Performance Standards	S$500 for every hour that passes the RTO threshold
4	Failure to maintain the System at the System Availability Level of 99.5% or above	System Performance Standards	S$1,000 per calendar month for every month there is a failure to maintain the System Performance Standards
5	2 or more occurrences of identical or similar failures of the System (as determined by e2i) within each calendar month during: (i) any of the Delivery Phases; or	Provisions of the Contract	S$2,000 on every occurrence of similar failure

	(ii) the Maintenance Phase (if any).		
6	Failure to meet the Service Levels for any Severity Level 1 or Severity Level 2 incident as defined	Incident Response and Resolution Times in Clause 9.3.2	S$2,000 for every occurrence
7	Failure to meet the Maintenance Service Levels for any Severity Level 1 or Severity Level 2 incident as defined	Incident Response and Resolution Times in Clause 3	S$2,000 for every occurrence

9.4. ESCALATION PROCESS

9.4.1. The Tenderer shall follow the escalation guidelines specified with the e2i's Quality Management System (QMS) escalation procedure via electronic mail or telephone/ SMS. The escalation procedure shall be given to The Tenderer upon award of the contract.

9.4.2. For problem under Severity 1, The Tenderer shall inform the e2i immediately through escalation process and shall brief the e2i on the causes, area of impact and lead-time for recovery within the response time specified in Clause 9.3.2.

9.4.3. The Tenderer shall note that the severity of a problem may be escalated based on circumstances such as high impact to user's operations. The e2i reserves the right to vary the recovery time when the need arises.

9.4.4. The Tenderer shall notify the e2i's Helpdesk when any application system is not available due to application problems.

9.4.5. The Tenderer shall escalate any Infrastructure problems back to the relevant e2i's Helpdesk if the problem is determined to be caused by the Infrastructure.

9.4.6. Currently, e2i monitors the effectiveness of e2i's Helpdesk based on the mis- escalated calls to The Tenderer. Mis-escalated calls are defined as answers found in the Frequently Asked Questions (FAQ) prepared by The Tenderer. The Tenderer shall assist the e2i by providing the necessary information on mis- escalated calls.

9.4.7. The Tenderer shall attend meetings with the various e2i's Helpdesk Managers if there is system instability or whenever there is a need to close up the escalation gaps between The Tenderer's Helpdesk and the e2i's Helpdesk.

9.4.8. The Tenderer shall attend meetings initiated by e2i together with the e2i"s Helpdesk to discuss on the major problems or issues encountered by users.

9.5. PROBLEM MANAGEMENT SYSTEM

9.5.1. The Tenderer shall propose a Problem Management System to enable its staff to log, update and track the status of the problems and major support activities.

9.5.2. Where problems are communicated to The Tenderer through the Helpdesk or via telephone or electronic mail from the e2i user directly, The Tenderer is expected to log all such problems reported into the Problem Management System and shall respond to the problem as stipulated in Clause 9.3.2.

9.5.3. The Tenderer's helpdesk shall provide incident numbers to the users or e2i"s Helpdesk who has reported the problems.

9.5.4. The e2i may from time to time request The Tenderer to locate specific type of problems or Helpdesk calls logged by specific users. The Tenderer shall be able to extract and print this information from the Problem Management System.

9.5.5. For any problems/defect and resolution, the e2i's Representative shall be updated of its status according to the timing specified in Clause 9.3.2.

9.5.6. All problems/defects shall be tracked. There must be proper acknowledgement of all reported System errors and encountered problems and monitoring of the status of the reported errors and problems by The Tenderer.

9.5.7. The Problem Management System shall be able to capture the following information:

(a) Caller information (Name, Department, Telephone number, Location, Email address)

(b) Date and time of user/ User Helpdesk call

(c) Type/Category/Sub-category of problem

(d) Problem description

(e) Details of problem resolution

(f) Date and time of response

(g) Date and time of problem resolution

(h) Date and time of problem closed

(i) Severity of problem

9.5.8. The Tenderer shall also provide an analysis of the problems encountered and propose actions to prevent these problems from recurring and pre-empt similar problems from occurring.

9.5.9. The Tenderer shall be measured on its Service Level for production support via the Problem Management System.

9.5.10. The Problem Management System shall be made available to the e2i"s Representative as and when needed.

10. TRAINING AND KNOWLEDGE TRANSFER

10.1. GENERAL REQUIREMENTS

10.1.1. When requested by the e2i, The Tenderer shall conduct training classes on any of the applications systems under this Contract. The training classes could be refresher (advance or novice) courses or introductory courses for new staff. Training for enhancements applied during the Contract Period shall be included in the Change Requests.

10.1.2. The Tenderer shall provide training to meet three (3) main objectives:

(a) To enable all users and nominated personnel to operate and use the System effectively.

(b) To enable all nominated technical personnel to operate and maintain all the system's software.

(c) To enable a smooth transfer of knowledge from The Tenderer to the nominated technical personnel on the project.

10.1.3. All training shall be conducted on site or in premises to be supplied by the e2i.

10.1.4. The Tenderer shall provide suitable and adequate customised training for staff or first line support (e.g. the e2i's Helpdesks) nominated by the e2i to enable them to carry out smooth operation and management of the System. The training provided shall include training on all software, products and services included in the System.

10.1.5. As and when needed, The Tenderer shall provide a full and comprehensive training proposal. This shall include courses to be conducted, course contents, cost per person,

class size, time table(s), course contents, trainee pre-requisites, duration of each course and instructors' resume.

10.1.6. The e2i reserves the right to accept part or all of the training courses and The Tenderer may be required to make the necessary amendments to the training courses and training materials wherever necessary.

10.1.7. The Tenderer shall be responsible for setting up the entire Training environment of the system. If needed, The Tenderer shall provide all necessary training equipment that is not currently available in e2i for these training purposes.

10.1.8. The medium of instruction and training document shall be in English. The Tenderer shall provide each trainee with a complete set of training documents and materials for his retention.

10.1.9. For every course conducted by The Tenderer, all training materials (hard and soft copies) shall be made available to the e2i. The e2i shall have the right to reproduce and use these training materials to conduct in-house courses for its personnel.

10.2. COMMUNICATION PLAN

10.2.1. The Tenderer shall, in consultation with the e2i, undertake the responsibility to define and implement appropriate Communication Plan for the various groups. The Communication Plan shall include:

(a) General users

(b) Senior management

(c) Third party Contractor(s)

(d) Sub-Contractor(s)

10.2.2. The Tenderer shall anticipate possible interfacing issues and undertake to work with and ensure that the third-party contractor(s) are sufficiently briefed on the scope of services and that their roles and responsibilities are clearly defined.

10.2.3. The Tenderer's responsibilities shall include the preparation of presentation materials, publicity brochures, briefings, and any other information. In some cases, The Tenderer shall provide the materials and assist in conducting the briefing sessions to the e2i's senior management and key users.

11. DOCUMENTATION

11.1. GENERAL REQUIREMENT

11.1.1. The Tenderer shall ensure that proper documentation of the System configurations, the changes made and the reasons or rationale for change are recorded for traceability.

11.1.2. The Tenderer shall provide all documents written in English and expressed in clear, consistent, readily understandable, and defined terms.

11.1.3. The Tenderer shall supply sufficient documentation and training manuals including, but not limited to the following:

(a) Application Software documentation

(b) User/training guide

(c) Document Control Documentation

(d) Any other documents, that The Tenderer shall supply, as specified in this tender

11.1.4. In addition, The Tenderer shall produce and adhere to the following mandatory documentation throughout the development and maintenance stages:

(a) Quality Assurance Plan

(b) Configuration Management

(c) Quality Review Records

11.1.5. e2i reserves the right to reproduce any documentation supplied with the System for its own internal use.

11.1.6. The Tenderer shall provide all documents in complete, accessible and readable form within seven (7) days from the Go-Live Date. The Tenderer shall provide time to time copies of the documents containing sufficient up-to-date information for the proper use and maintenance of the system (current). These documents may be supplied in electronic form.

11.1.7. The Tenderer shall provide any revised editions, supplementary materials, or new publications relevant to the System at no extra cost to e2i.

11.1.8. The Tenderer shall provide draft versions of the documentation for e2i's review if requested before delivering the final version of the documentation to e2i for approval. The Tenderer shall cater for at least two (2) calendar weeks for each review.

11.1.9. e2i shall accept the final version of the documentation, after all the corrections have been made and after all amendments required by e2i have been incorporated into the documentation by The Tenderer.

11.2. APPLICATION SYSTEM DOCUMENTATION

11.2.1. The Tenderer shall provide complete and thorough documentation for all proposed or supplied application software / services.

11.2.2. The Tenderer shall provide the following documents:

(a) Project Plan

(b) Design Specifications

(c) System Test Plan

(d) System Test Report

(e) User Acceptance Test (UAT) Plan and Test Cases

(f) User Acceptance Test (UAT) Report

(g) Performance Test Plan

(h) Load and Stress Test Report

(i) Installation Guide/Manual

(j) Operation Guide/Manual

(k) System implementation document (e.g. Functional requirements specs, gap analysis document, etc)

(l) Technical documents (e.g. Technology infrastructure, solutions stack, interface documents, etc);

(m) Any other documents, that The Tenderer shall supply, as specified in this Tender

11.3. USER/TRAINING GUIDE

11.3.1. The Tenderer shall provide complete and detailed documentation to ensure effective use of the System by the users. The documentation shall include the following:

(a) Overview of the System

(b) Policy and objectives of the System

(c) Processes supported by the System

(d) Description of functions, screens, reports, processes

11.3.2. The Tenderer shall ensure that all documentation for the users are detailed / described from the user's perspective and shall include practical examples and comprehensive indexes to facilitate quick reference.

12. EXIT PLAN

12.1 The Tenderer shall propose and submit an Exit Plan to cover the termination of the contract. The Exit Plan and the detailed schedule shall be subject to e2i's approval.

12.2 e2i will provide sixty (60) days' advance notice for the termination in writing.

12.3 The Tenderer shall be responsible for conducting a detailed handover, inclusive of briefing and training sessions, of the complete System to e2i and the next Contractor. Any cost incurred during the period of hand-over will be borne by The Tenderer. The handover shall be conducted concurrently with the ongoing support required of The Tenderer without affecting the Service Levels.

12.4 The Exit Plan shall include but is not limited to:

(a) Processes and procedures to:

i. Uninstall all software that was installed and configure at the Local Sites for the use of the System

ii. Hand over all necessary documentations

iii. Hand over all records of problem logs and their resolution status

iv. Hand over all files and data, including user account details and user data

v. Perform secure erasure on the storage media of the servers to remove all data from the System. The Tenderer shall ensure that unauthorized personnel are unable to recover any data on the storage media.

(b) Roles and responsibilities of:

i. The Tenderer and e2i

(c) Detailed schedule with clear milestones

(d) Documentation of the System/Application should include the following:

i. Detailed Design Specifications

ii. Program Specifications

iii. Program Source Code

iv. Installation Plan

v. Configuration Management Document of Database, Operation Systems and other system software

vi. System Administrator / operations procedures

vii. System start-up and shutdown procedures

viii. System error messages and diagnostics

ix. System backup and archival procedures

x. System failure and recovery procedures

xi. Monitoring and managing system security

xii. Capacity planning, system performance monitoring and tuning

xiii. Conceptual system architecture

xiv. Operational procedures within the participating organisation

xv. Description of functions, screens, reports, processes

xvi. System interfaces

12.5 The Tenderer is to assist e2i to conduct exit audits and ensure all the requirements in the contractual agreement is fulfilled.

12.6 The Tenderer is to ensure any data migrations or transfers to the new vendor is done securely.

12.7 The Tenderer to ensure that their access to e2i's IT systems and databases is terminated on or before the last day of the contract.

12.8 The Tenderer is to assist e2i to ensure the return of all IT assets, computing devices, documents and access passes to e2i on or before the last day of the contract or engagement.

12.9 The Tenderer is to return or destroy all e2i's personal data within the stipulated timeframe and confirm in writing to e2i that it has destroyed the said personal data.

12.10 The Tenderer is to document all work done and deliverables fulfilled in a project closure report or end-of-engagement report.

12.11 Any extra costs incurred for execution of the Exit Plan shall be borne by the Tenderer.

12.12 The exit transition period shall be managed and supervised by e2i.