27 FACIAL RECOGNITION BIOMETRIC AUTHENTICATION SYSTEM

27.1 Overview

27.1.1 As part of the industry productivity initiative and in line with the latest Building Control (Buildability) Regulations, the Building Construction Authority (BCA) collects productivity and other related data of construction projects on a regular (monthly and other period) basis using the Electronic Productivity Submission System (ePSS).

27.1.2 The Authority intends to deploy Facial Recognition Biometric Authentication System (FRBAS) for the purpose of manpower data collection and thermal/temperature scanner to detect fever symptoms and mask detection in CR206 for the purpose of manpower data collection and to deny entry to people with above specified temperature.

27.2 Definitions

Unless otherwise stated, the meaning and explanation of the terms below apply to this Contract.

27.2.1 “System” means all hardware, software, middleware, application software forming part of the System including the Frontend user service (biometric facial recognition reader, thermal imaging/temperature scanners, etc.) with interfaces to the Backend application (cloud hosting services, database, etc.), the hosting necessary for manpower data collection at all entry and exit locations at CR206, a Web-Based Integrated Manpower Data and Tracking Management and Reporting function.

27.2.2 “Operations & Maintenance Specification” means the Software Support and Hardware Maintenance Specification contained herein that govern the operation, corrective maintenance and preventive maintenance of the Hardware and Software for the System.

27.3 Scope of Works

27.3.1 The scope of works shall include, but not be limited to, the following:

27.3.1.1 Design, supply, install, test and commission all new hardware, equipment and software necessary for a FRBAS for manpower data collection at all entry and exit locations at the construction site and a Web-Based Integrated Manpower Data and Tracking Management and Reporting function (“System”);

27.3.1.2 Generate the necessary manpower data and output in the required format and upload to the BCA's ePSS;

27.3.1.3 Provide body thermal imaging/temperature scanning sensor and mask detection compatible with the System. If fever is detected and/or any person not wearing masks, the reader shall sound an alarm and System will deny access to the individual;

27.3.1.4 Provide comprehensive operations and maintenance services for the System in accordance with the Specifications and the Operations and Maintenance plan; and

27.3.1.5 Upon completion of the works, to decommission, dismantle and remove the System as directed by the Engineer and to archive and transfer the entire database to the Authority according to the approved Exit Plan.

27.4 General

27.4.1 The Contractor shall provide a complete system including all the necessary hosting, hardware, system software, middleware, application software and professional services to fulfil the objectives and requirements as outlined in the Specifications.

27.4.2 The Contractor shall provide a detailed breakdown of the Bill of Materials (BOM) for the System. The BOM shall minimally include the cloud sizing, cloud instances, software listing, on-site hardware listing and quantity.

27.4.3 The Contractor shall indemnify the Authority against all costs, charges, expenses and the like resulting from his failure to properly co-ordinate, carry out, install, commission and complete the Works as required under the Contract.

27.4.4 In the event the Engineer deems that the progress of the supply and installation of the FRBAS is slow to meet the construction works schedule/programme, the Engineer will issue a written notice to the Contractor to increase his resource level as necessary to meet the schedule and all such increases in resources shall be deemed included in the Contract Price.

27.4.5 The Contractor shall allow in his Contract Price the shifting of the FRBAS and re-installation of the System as and when required by the Engineer. The Contractor shall ensure that no data is lost during this transition period.

27.4.6 The relocation cost shall include:

a) Flap barrier gates and readers installed on removable steel platform to enable modular shifting of biometric gate components and accessories by the Contractor to another site; and

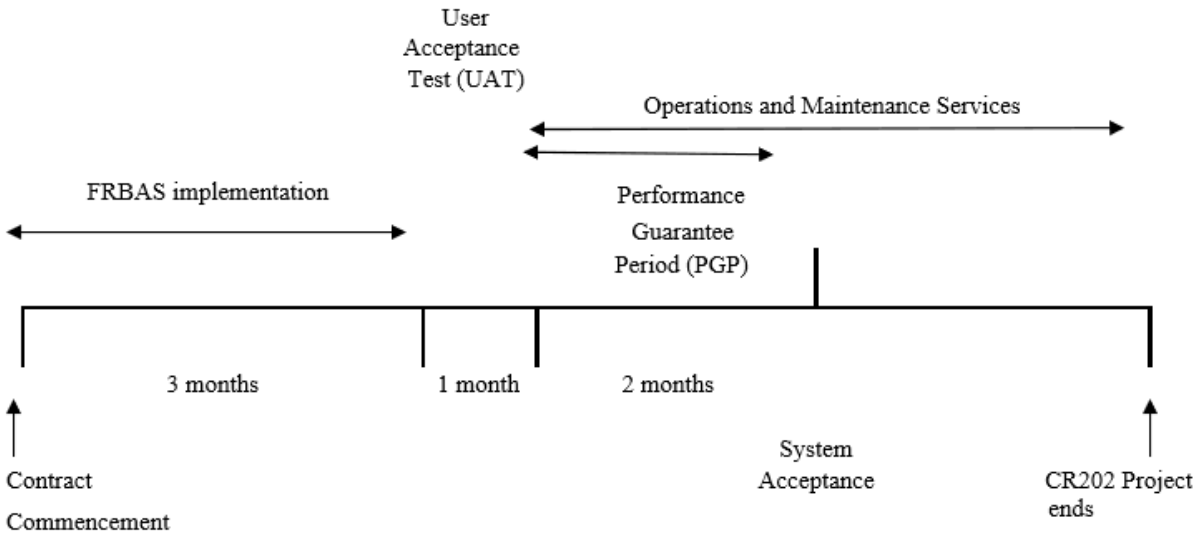
b) The Contractor shall set up and commission another operationally ready flap barrier gates and readers before the new site/location is operational, in the event that the existing set cannot be relocated to the new site/location.

27.4.7 The Contractor shall allow in his Contract Price the provision of any additional FRBAS to cover any new and/or additional entry and exit locations that may arise during the contract period, subject to the Engineer's acceptance.

27.5 Project Schedule

27.5.1 The Contractor shall propose a Project Schedule detailing all project tasks and a detailed plan for the roll-out of the System to the Engineer for acceptance.

27.5.2 The project schedule is described below:



27.6 User Acceptance Test (UAT)

27.6.1 The Contractor shall ensure the successful completion of system integration prior to commencement of the UAT on site.

27.6.2 The Contractor shall plan for in his programme at least one (1) calendar month for the UAT.

27.6.3 During the UAT period, the Contractor shall rectify all defects at a mutually agreed timeframe with the Engineer.

27.6.4 The Contractor shall fulfil the exit criteria requirements (System meeting all functional and technical requirements in the Specifications) for the UAT before UAT can be considered completed.

27.6.5 Upon the completion of UAT, the Contractor shall submit the necessary documentation, for the Authority's approval to proceed for System Commissioning. This shall include an action plan to resolve any outstanding issues.

27.6.6 Upon successful completion of UAT, the Contractor shall obtain a UAT sign off.

27.7 Installation and System Commissioning

27.7.1 The commissioning of the installed System shall be subject to the completion of the following:-

a) All known defects have been rectified;
b) All known significant risks have been mitigated and appropriate risk management strategy has been implemented; and
c) Completion of the housing structures.

27.8 Performance Guarantee Period (PGP)

27.8.1 The PGP shall commence after the Commissioning Date and continue for a period of two (2) calendar months.

27.8.2 The Contractor shall monitor the System and fine-tune the System to achieve optimum performance and system availability, including all connected equipment.

27.8.3 During PGP, the Contractor shall be responsible to log all faults encountered, investigate, and present the findings and proposed rectifications to the Engineer, and rectify the faults. Any defects that occur during PGP shall be promptly fixed by the Contractor solely at the Contractor's Price.

27.8.4 The Contractor shall review the System Performance and substantiate the completion of PGP with system performance report including statistics of system availability for the System during PGP.

27.8.5 During the PGP, the Contractor shall provide comprehensive operations and maintenance services in accordance with the Operations and Maintenance Specification.

27.9 Acceptance Date

27.9.1 The Authority shall accept the System only upon the successful completion of Performance Guarantee Period (PGP).

27.9.2 The Contractor shall review the System Performance and Capacity Utilisation and substantiate the completion of PGP with system performance report including statistics of System Availability for the System during PGP.

27.10 Documentation

27.10.1 The Contractor shall submit a detailed proposal for the Engineer's acceptance which shall include but not limited to the following: details of the System, site utilisation plans showing the proposed location(s) of the System to capture all the manpower data required (including site office(s), site storage area(s) etc.), installation method and ability of the System to track each worker to derive the manpower data for uploading onto ePSS.

27.10.2 Work sessions (defined to be meetings between the Engineer and the Contractor) may be arranged as and when required to understand the requirements, resolve project-related issues and review the documentation and design of the System. The Contractor shall be responsible for updating the documentation should there be any missing gaps discovered in the course of the Contract.

27.10.3 The Contractor shall provide at least ten (10) working days, or otherwise specified by the Engineer, for the Engineer to review the designs and documentation when required. The Contractor shall also incorporate any amendments and ensure completeness to the designs and documents within five (5) working days and resubmit to the Engineer for final review. The designs and documentation shall not be deemed as complete until accepted by the Engineer.

27.11 Co-ordination and Interfacing with Authority-Appointed Consultants/Contractors, System-Wide Contractors

27.11.1 The Contractor shall be responsible for the co-ordination with all parties for all works and services related to the System. These parties shall include, but not limited to the Authority, the Authority's Project Team, QP(S) Team, Instrumentation & Monitoring Contractors, Accredited Checkers and System Wide Contractors (SWCs) who are using the System. These Interfacing Contracts may commence before or during the period of this Contract. No claim will be accepted for such

coordination and interfacing with additional contractors or other parties not previously identified.

27.11.2 In the event that the Contractor and Interfacing Contractors do not agree on the co-ordination of the works, the Engineer's decision shall be final. The Contractor shall not be entitled to claim for any time and cost incurred arising from this.

27.12 Exit Plan

27.12.1 The Contractor shall propose and submit an overall exit plan on the conversion, transfer and/or deletion of the database to the Authority upon the end of the CR206 project. The exit plan shall be submitted within twelve (12) months from the Contract Commencement Date to the Engineer for acceptance.

27.12.2 The exit plan shall elaborate how the existing database would be transferred into readable and self-contain format (e.g., Microsoft Access DB, Excel), and the data that are included (e.g., master data, personnel records, reporting data, etc.) or excluded (e.g., transactional entry/exit data) as part of the data transfer.

27.12.3 As part of the exit plan, the Contractor shall ensure that all Contractor owned media (disk drives, tapes, etc.) containing Authority's information assets are securely erased and sanitised.

27.13 Provisions for the System

27.13.1 The Contractor shall provide the following for the System:

	Location	
1	Biometric enrolment station at contractor's site office	To provide a dedicated air-conditioned room to house the FRBAS enrolment station complete with a) Electrical lightings; b) Four (4) 13A twin power sockets; c) Office desk with cable management system and chair; d) Desktop computer (Windows Operating System and web browser included) and LCD monitor and HD web cam for registration purpose; e) Network cabling connection with Broadband internet access; and

		f) Uninterrupted Power Supply/Back up battery for desktop computer.
2	Biometric facial recognition reader with thermal imaging/temperature scanner unit at QPS staff's office	a) To provide four (4) 13A twin power sockets; and b) To provide network cabling connection with broadband internet access.
3	Biometric facial recognition reader with thermal imaging/temperature scanner unit at each site ingress/egress gate	Fixed Site Ingress/Egress Gate Location To provide a sheltered enclosure for the FRBAS site ingress/egress gates and a security guard post or CCTV monitoring unit (for remote site); or Unfixed Site Ingress/Egress Gate Location To provide a sheltered 10ft x 8ft open concept container for the FRBAS site ingress/egress gates and a security guard post or CCTV monitoring unit (for remote site) complete with: a) electrical lightings & switch; b) 4 nos 13A twin power sockets; c) ELCB/MCB board with junction box; d) roof shelter with insulation; e) painted chequered plate flooring; f) lightning protection system; g) interior and exterior painting; h) sheltered partitioned walkway; and i) PE endorsement

27.13.2 The Contractor shall submit his design of the sheltered enclosure and/or protection housing for the engineer's acceptance, taking into account the position of the system reader design in his design such that the performance of the System will not be affected by lightning and weather conditions in the normal operation of the System, in particular the biometric readers.

27.13.3 The Contractor shall protect the System against any damage or loss from vandalism, fire, weather condition, mishandling, water, theft, power outage and not to tamper with and/or change the configuration of the

System. In the event of loss or damage to the System, the Contractor shall indemnify the Authority of any costs and expenses incurred in repair, keeping the access control system equipment in good condition and working order or the replacement of the System equipment or any part thereof.

27.13.4 The Contractor shall ensure that the computer designated as the access control system enrolment station shall not be used for any purpose other than for registration.

27.13.5 The Contractor shall provide stable power supply and network infrastructure.

27.13.6 The Contractor shall ensure all user records, especially those designated as mandatory fields, are inserted.

27.13.7 The Contractor shall carry out periodic maintenance of user records by deleting records of inactive users and purging obsolete user records.

27.13.8 The Contractor shall record and update the site work quantities done into the access control system for the respective trade level/project level data on a monthly basis or at other intervals as required by the Engineer.

27.14 General Functional Specifications

27.14.1 The System shall function to monitor the manpower under their respective trade, skill or profession and generate the required data or output in the required format and uploaded into BCA's ePSS. The implemented System shall track the movement of each worker (general workers, skilled personnel and site management staff etc.) entering and exiting the construction site according to the trade type, the working hours per day of each worker and the man-day on Site.

27.14.2 The Contractor shall operate the System to monitor and track the manpower deployed for all construction works under the CR206 contract and carry out the submission of manpower deployment data to BCA through the ePSS.

27.14.3 The System shall be capable of generating manpower report in various formats including Microsoft Excel or PDF format including manpower report which shall be submitted by the Contractor to BCA at monthly intervals or other frequencies as and when required by the BCA. The manpower reports generated by the System shall be protected from deliberate editing and tampering till they reach BCA's ePSS systems.

27.14.4 The System shall be protected against unauthorised editing of collected manpower tracking data, virus or malicious software etc. which may otherwise corrupt the System.

27.14.5 The System shall have the ability to transmit the manpower report directly from the System to BCA's ePSS in addition to file uploading separately.

27.14.6 The System shall allow to record and manage information concerning all workers and companies including that of System Wide Contractors, Instrumentation & Monitoring Specialist, Qualified Person (Supervision) including the Qualified Site Supervisors within a construction site.

27.14.7 The System will be used by the Authority to record the daily, weekly and monthly attendance of the Qualified Person (Supervision), QP(GEO), Specialist Supervisors and Qualified Site Supervisors for payment certification purposes. It shall be capable of generating detailed timesheets for QP(S) personnel to submit to the Authority's Project Administrators for endorsement or rejection back to QP(S) personnel for further amendments before resubmission. The System shall have the facility to allow amendments to the template of the timesheet at the request of the Engineer for his acceptance. The Contractor shall be deemed to have allowed for this requirement in his Contract Price.

27.14.8 The proposed System should be proven in other projects with similar setup and records.

27.14.9 The System shall come with sufficient backup facilities to safeguard the manpower database so as to enable the data to be called up anytime for the purpose of reporting to the user's management.

27.14.10 The System shall be equipped with suitable measures (e.g. backup battery supply) to ensure the integrity of the manpower monitoring data is not affected during power outage.

27.14.11 In the event of system breakdown, alternative means shall be proposed by the Contractor to continue to monitor and track the manpower under their respective trades. The Contractor shall carry out the necessary repairs and/or replacements of faulty components so that the System can resume operation.

27.14.12 In the event of a faulty reader, thermal/temperature scanner and/or turnstile flap barrier gates, the Contractor shall propose alternative such as QR code or other means to ensure no interruption to the operations.

27.14.13 The Contractor shall comply with the following policies, standards, guidelines and best practices that may be issued by the Government or the Authority. A copy of the relevant documents will be provided for viewing upon request. These include:

a) Government Instruction Manual for IT Management (IM8);

b) Policy for Systems using Commercial Clouds; and

c) LTA Data Management Policies & Guidelines.

27.15 System Architecture & Support

27.15.1 The Contractor shall ensure the System includes the following features:

27.15.1.1 The capability to:

a) Achieve a maximum clearance processing time of 1 minute for every 10 persons passing through each of the controlled access location;

b) Handle data transactions of an up-dated listing of active System users (up to a maximum of 15,000 users). The System shall also be able to detect and automatically remove any dormant users from the active users list and to revoke the gate entry access of these users after reaching a specific duration defined by the Authority; and

c) Store a minimum of 4000 facial templates per biometric reader.

27.15.1.2 Dedicated secure web services with high availability and redundancy of database / application servers (to meet the System availability of 99%) using Extended Validation (EV) digital certificates;

27.15.1.3 Enterprise Server (Centralised Server that replicates data from the controllers at the CR206 site) shall be cloud hosted in Singapore with round the clock support, data security management and redundancy for internet and power services and without dependency of the site office network infrastructure.

27.15.1.4 The server resources shall be capable of supporting concurrent users (minimum 15 users), software and functions and meet the following requirements:

a) Shall be scalable, high availability, dedicated and with full disaster recovery system backup and restore solution to achieve Zero data loss;

b) Shall have redundancy features that allows switchover of operations for critical equipment should it fail to function; and

c) Shall be of easy serviceability without the need to shut down the System or affecting the System operation.

27.15.1.5 Provision of local access/egress controllers at the entry/exit gate gantries in the event that Enterprise Servers are down, the system shall continue to perform access control management. The Controller on field that controls the gate gantries shall be highly reliable and shall have its own transaction and alarm logs backup in its internal memory. In the event that network between the controllers to the server fail, the controller at various gates shall have the capability of buffering all data and send to the server once the network has restored;

27.15.1.6 Power system redundancies to the System;

27.15.1.7 The System shall have the capability to handle consistency network issue (including momentary drop signals by telco) to keep the data flowing through;

27.15.1.8 Web based registration of users (workers / LTA staff / QP(S) / the Contractors' staff / System Wide Contractors' staff / IM Contractors' staff) for gate access is done at dedicated site office;

27.15.1.9 Capable of designing any form of reports and visual presentations (spreadsheet or graphical) that can be viewed on various platforms including computer consoles, handphones, tablets, etc., and for hardcopy printing;

27.15.1.10 A Customisable Graphic User Interface (GUI) platform that would allow the user to call out any information available within the System (for example, a search function which calls out the manpower data, status of any personnel on site, etc.) required by the Authority. The proposed illustrations within the GUI shall include text, graph and photos. The layout shall be submitted to the Engineer for acceptance;

27.15.1.11 Data entry

a) Manpower record entry – Allows the Contractor / LTA Administrator(s) to key in/edit a manpower record for registration purpose;

b) Construction Statistics - Allow the Contractor / LTA Administrator(s) to regularly key in/edit:

i. Quantities for site work done for the various trades for the purpose of monitoring the productivity of the workers based on trade-level productivity indicators for the purpose of measuring productivity; and

ii. Workers numbers based on the Contractor's Manpower Resource Histogram for the purpose of **Clause 27.15.1.16**.

27.15.1.12 The System shall be designed with great flexibility to allow for changes e.g. adding additional customized fields and to allow the System administrator(s) to update any input field e.g. changes to trade classification, or skill status, e.g. R1/R2, etc. without inadvertent overwriting of the earlier manpower records based on the previous input fields unless such manpower record overwrite is accepted by the administrator;

27.15.1.13 The System shall allow the same users to register at multiple construction sites with no or minimum re-registration efforts of the user's biodata required. However, the System must be able to reflect and highlight the multiple entries by the same user at different construction sites in the report;

27.15.1.14 It is possible that user may register different trade classification, or skill status at different construction sites. The System shall be required to accurately capture the user's manpower records based on the respective trade classification or skill status e.g. R1/R2 registered by the user at the respective construction sites;

27.15.1.15 User-friendly. For example, the System should incorporate meaningful error messages, pull-down menu and on-line help features; and

27.15.1.16 The capability to authenticate man-hours and generate report on specific RC trades for the duration of RC works to assess the Contractor's compliance with the Manpower Productivity Requirements (R1 >30%, R2 with 4 years of experience >55%). Refer to the relevant extract of the Contract provisions on Manpower Productivity Requirements in **Clause 4.3** of the Particular Specification.

27.15.1.17 The System shall have a built in contactless thermal imaging/temperature scanner and meets the following minimum requirements:

a) Provide real time warning in the event of temperature abnormality and if detects person that is not wearing masks.

b) Temperature Range 30 Deg C to 45 Deg C with accuracy of ± 0.3 Deg C at a distance of 0.5m to 2m;

c) Authentication Speed of less than 1 sec;

d) False Acceptance Rate (FAR) of less than 0.001%;

e) False Rejection Rate (FRR) of less than 1%;

f) Reminder to wear Mask Detection with an alert for pass/fail authentication; and

g) 7” TFT Display

27.15.2 The Contractor shall ensure that all accounts used in the System are able to be set with an expiry date.

27.15.3 The Contractor shall implement the following features when using password as the means of authentication.

a) Enforce passwords to be made up of at least 12 characters and contain characters from at least two of the following four categories

i. Upper case (A through Z)

ii. Lower case (a through z)

iii. Digits (0-9) and

iv. Special Characters (!, $, #, %, etc.)

b) Enforce password change once every twelve (12) months;

c) Prohibit password reuse for a minimum of three (3) generations;

d) Ensure passwords are not displayed in clear;

e) Transmit only cryptographically protected passwords;

f) Store passwords in a form that is resistant to offline attacks;

g) Enforce password change upon the first login;

h) Prohibit passwords from being the same as the account ID or user ID;

i) Limit consecutive failed authentication attempts that can be made on a single account to 10 times or less; and

j) Protect the system against dictionary or brute-force attacks.

27.15.4 The System shall support data encryption using Advanced Encryption Standard (AES) with minimum 256-bit keys.

27.15.5 The Contractor shall provide the necessary processes and procedures to authenticate all work hour records input in the System and establish a mechanism to capture the additional working hours in excess of the allowable maximum hours of work under the prevailing MOM statutory ruling on workhours. The Contractor shall incorporate feature(s) in the System to clearly define and highlight any additional working hours for administrative purposes and generating report showing the overtime hours based on an approved template for QP(S) personnel to submit to the Authority's Project Administrator(s) for record.

27.15.6 User System Access Rights

27.15.6.1 All information available to the users shall be controlled using user profile for different level of users. Example, master administrators shall have the highest user rights accessing and controlling information across the entire network. This user shall have the right to grant or restrict other user assessing the system. The user rights and information available to different users shall be proposed and is subjected to the Engineer's acceptance.

27.15.6.2 A preliminary concept of the security levels is shown below. After the award of the Contract, the Contractor shall work with the Engineer to finalise the required security levels.

a) LTA Master Administrator: all functionalities of the System including giving access rights to LTA / Contractors' Administrator.

b) LTA Administrator: entry, enquiry and retrieval of all records and reports but restricted based on assigned Contract(s).

c) The Contractors' Administrator: entry and enquiry of all records and granting/revocation of manpower site access but restricted based on assigned Contract(s).

d) Refer to **Appendix PS-27-A**.

27.15.6.3 Allow on-line creation and assignment of user security access.

27.15.6.4 Allow on-line creation and deletion of user to a specific group of contracts and/or projects.

27.15.6.5 Allow to generate master files records and reports related to the Access rights as defined in the System for example listing of users' access, staff notification list, etc.

27.15.6.6 The Contractor shall establish standard operating procedures to make sure that the account and access rights of user and external parties are updated in a timely way. Frequency of the review shall be:

a) All accounts – Annually;

b) List of inactive/suspended accounts – Monthly; and

c) List of staff who has left, redeployed or changed job role – Monthly.

27.15.7 Establishment and Maintenance of Master Files

27.15.7.1 To enable the System administrator to assign coding for subsequent data trend monitoring and analysis, the System shall allow the administrator to establish and maintain Master Files for coding. The Master Files include but not limited to the following:

a) Trades;

b) Man-days;

c) Construction Statistics;

d) Worker's classification;

e) Contracts;

f) Contractors/Sub-Contractors;

g) Qualified Person (Supervision) (QP(S));

h) System Wide Contractors; and

i) Manpower Biodata.

27.15.8 Data Query and Report

27.15.8.1 The System shall provide a one-stop resource-efficient, secure & 2 Factor Authentication (2FA) via SMS enabled web-based portal for

quick retrieval of information on productivity performance trends within CR206. SMS charges shall be deemed included in the Contract Price. The System shall allow analysis of system information and generation of printable reports to suit various functional and management needs in the following areas:

a) Manpower database of LTA contractors and subcontractors (Information on R1, R2, Man-Year Entitlement (MYE), MYE waiver cases, etc.);

b) QP(S) daily/weekly/monthly timesheet records;

c) Productivity statistics and trend analysis (e.g. Project/Contract Level and Trade Level Indicators);

d) Productivity performance trends of the Contractor and sub-contractors;

e) Monthly Productivity performance on CR206;

f) Annual CR206 project performance on productivity improvements;

g) Raw Core Trade Personnel Deployment List;

h) Assessment of the Contractor's compliance with the Manpower Productivity Requirements; and

i) Monthly Raw Manpower Data Report.

27.15.8.2 The System shall be able to generate reports filtered by any of the available field values (Refer to **Appendix PS-27-B** for examples of Output Screen Display/Report).

27.15.9 The Contractor shall carry out System performance checks to ensure optimum availability of the System.

27.15.10 The Contractor shall provide professional services for the following:

a) Submission of System Design proposal, Test and Commissioning plan, Installation Plan, Installation methodology & design for the Engineer's acceptance;

b) Security assessment and testing;

c) Setup, install, configure, test and commission the System;

d) Lead and coordinate with other contractors for the seamless implementation of the System; and

e) Provide documentations on the installation, configuration, testing and commissioning of the System.

27.15.11 The Contractor shall ensure that the Hardware and/or Software for the System shall have the following support:

a) Local presence, local logistic and on-site support for the hardware/firmware/software;

b) Local phone supports for the Authority or interfacing contractors to log call/resolution on software and hardware issues;

c) Support: technician/engineer with unlimited tech support and call centre hotline; and

d) Services co-ordinator shall be appointed to install, configure, maintain software, Operating System & hardware and to monitor systems/manage disk allocation/ back-ups; handle database admin work, etc.

27.15.12 The System Software support shall cover unlimited phone support, free version upgrades, bug fixes and patches.

27.15.13 The Contractor shall provide product documentation and details on the features and functions of the Hardware and Software.

27.15.14 Hardware fault in any of the peripheral and/or software error in a subsystem shall not lead to total system failure. The Software and Hardware shall be fully tested prior to implementation in order to ensure a maximum level of reliability of the components.

27.15.15 The Contractor shall be responsible to rectify the defect or replace part or whole component if the defect surfaced from the System.

27.15.16 Hardware and System Software Delivery

27.15.16.1 Upon the delivery of Hardware and Software for the System, the Contractor shall prepare an inventory checklist for the items for the Hardware and Software delivered. The Engineer will verify the delivered items against the list. The Contractor shall ensure that all items of Hardware and Software are checked to be in working condition before assembly.

27.15.16.2 The Contractor shall provide services which include supply and delivery of all goods, unpacking, taking stock of the delivery, physical inspection for damages, site survey and proper disposal of all packing materials.

27.15.16.3 The Contractor shall provide the following information in the form of sticker which comes with strong adhesive tag or label on the front of the Hardware where it shall be clearly visible to Authority at all times:

a) Machine serial number;

b) Contactor's name; and

c) Contractor’s contact number

27.15.17 Installation and Configuration

27.15.17.1 The Contractor shall ensure that all the Software (including OS) are installed with the latest firmware and software patches before application and database installation.

27.15.17.2 The Contractor shall provide software/driver(s) of the latest versions at the time of implementation and the Contractor shall upgrade the software/drivers to the latest available versions during the contract period.

27.15.17.3 The Contractor shall be responsible for the configuration, sizing, installation, security settings, testing and the necessary setup to ensure smooth connection to the databases, successful publishing for dashboards and optimization of System performance in UAT.

27.15.17.4 The Contractor shall propose and implement a comprehensive system backup strategy including data retrieval strategy.

27.15.17.5 The Contractor shall ensure that all Hardware and/or Software are fully tested prior to implementation in order to ensure a maximum level of reliability of the components. The Contractor shall be responsible for implementing IT security measures including installing Anti-Virus software, updating latest virus definition files, installing security patches, running regular scans base on recommendation for software vendors to ensure optimization of System performance.

27.15.17.6 The Contractor shall be responsible to coordinate, liaise and work with the Original Equipment Manufacturers (OEMs) and/or sub-contractor(s) to resolve issues/problems that are related to the System.

27.15.17.7 All accessories such as cables, connectors and equipment required for the complete installation and functioning of the System shall be provided by the Contractor.

27.15.17.8 The Contractor shall implement the best practices/approach to setup and configure the server to protect the server resource and data from mishandling, unauthorised users and to achieve data integrity, confidentially and service availability.

27.15.17.9 The Contractor shall ensure that the supplied electrical cables comply with the Singapore Standards and the electrical cables are able to withstand the electrical loads required. The Contractor shall provide evidence of compliance to show that the electrical cables are able to withstand the environmental condition and electrical loading.

27.15.17.10 The Contractor shall tune and/or configure the Hardware and Software, ensuring that the System's performance is optimized.

27.15.17.11 All outdoor equipment and cabling shall be rated IP65 and the cable is of armoured type.

27.15.18 Data Connectivity

27.15.18.1 The Contractor shall propose suitable and reliable mechanism for fast, secure and easy data accessibility.

27.15.18.2 The Contractor shall ensure that data uploading and downloading from the biometric readers/controllers to the cloud hosted servers are transmitted in a secured manner.

27.15.18.3 The Contractor shall ensure that the System is able to connect to the database smoothly and the loading time shall be fast enough for dashboard refreshing and scheduled data updating.

27.15.18.4 The Contractor shall propose and implement appropriate controls to restrict direct connection to database to ensure the database performance is not adversely affected.

27.15.18.5 The Contractor shall propose suitable data connection solutions for scenarios which may occur during set up of System such as different dashboard sharing the same data source, big data source, etc.

27.15.18.6 The Contractor shall not use any wireless connectivity provided by the Authority.

27.15.19 Data Encryption and Authentication

27.15.19.1 The Contractor shall ensure that all passwords, user ids, and submitted documents are stored, and transmitted in encrypted form. The Contractor shall ensure that all proposed cryptographic software and algorithms remain secure and have not been compromised at the point of implementation.

27.15.19.2 The Contractor shall implement procedures to ensure that cryptographic keys are managed appropriately throughout its lifecycle, starting from key creation/generation, usage, backup, recovery, revocation to key destruction.

27.15.19.3 The Contractor shall ensure that all cryptographic module failures are logged.

27.15.19.4 The user authentication system shall have the following features:-

a) User identification shall be unique and identify the user;

b) Passwords must always be encrypted in storage using industry standard one-way hashing algorithms;

c) Auto-prompting for password changes upon first login shall be provided. Passwords shall only be known to the respective user, no system shall allow the viewing of passwords; and

d) Provide password expiration and shall alert the user a configurable time period (initially set to fourteen (14) days) before the password is due to expire.

27.15.20 Wireless Security

27.15.20.1 The Contractor shall ensure that the proposed solution has adequate security measures to ensure the confidentiality, integrity and availability of the data transmitted.

27.15.20.2 The Contractor shall ensure that wireless security is utilised and it shall be based on Wi-Fi Protected Access (WPA2) that does not have any known vulnerabilities, such as WPA Version 2 Enterprise Mode (802.11i) which is secure.

27.15.20.3 If WPA Pre-Shared Key (PSK) technology is proposed, passwords of minimum password length (of 32 characters without leading or trailing blanks) shall be used.

27.15.20.4 The solution shall have counter rogue access point (AP) capability.

27.15.20.5 Wi-Fi AP management shall be via secure means, with encryption supported.

27.15.21 General IT Security

27.15.21.1 The Contractor shall describe in detail all the security and access control features of the proposed solutions.

27.15.21.2 The Contractor shall ensure that its technical and security personnel are trained in IT security and are aware of the security implications of the work performed. The personnel shall be well-versed in the security requirements of the Authority as well as adhere to the changes of the security requirements by the Authority from time-to-time.

27.15.21.3 In cases where the policy and procedure requirements cannot be complied with, the Contractor shall be required to perform security risk assessment and propose alternative controls to address or mitigate the risks to a level that is acceptable by the Authority.

27.15.21.4 The Contractor shall ensure provision of necessary security features to guard against unauthorised access, intrusion, loss of information, software error and vulnerability to malicious attacks.

27.15.21.5 The Contractor shall ensure that the configurations of the systems are secured and reviewed before commissioning for Authority's use. This may include removing or disabling the unnecessary services or ports, system/user accounts and their access rights and system privileges on the various components.

27.15.21.6 The Contractor shall ensure that all data is encrypted At-Rest and In-Transit.

27.15.21.7 In an unforeseen event where a security breach has occurred, the Authority and/or Engineer reserves the rights to ask for hourly updates and resolution reports. The Contractor shall provide manpower who are experienced in dealing with such exigencies at no cost to the Authority. In case of a police investigation related to such security breaches, the Contractor shall cooperate with the Authority and relevant authorities during the investigation.

27.15.21.8 The Contractor shall ensure that all operating systems, databases, network devices, web and application software are configured and secured in accordance with latest version of established security guides (e.g. CIS Security benchmarks etc.).

27.15.22 Application Security

27.15.22.1 The Contractor shall adopt secure design, secure coding and secure testing practices to ensure that software is developed, tested and implemented securely.

27.15.22.2 The System shall enforce authorized access at information, system and application level.

27.15.22.3 All data input to the application shall be fully validated. This shall include:

a) Non-validated input (i.e. input field shall conform to the desired formats and values);

b) Broken access control;

c) Broken authentication and session management;

d) Cross-site scripting;

e) Buffer overflows;

f) Injection vulnerability flaws;

g) Race conditions;

h) Improper error / exception handling;

i) Insecure storage;

j) Denial of Service; and

k) Insecure configuration management.

27.15.22.4 Sufficient audit information shall be recorded to enable detection and investigation of security incidents.

27.15.22.5 The System shall notify the user, upon successful logon, of the date and time of the last logon.

27.15.22.6 Passwords shall not be hard coded into any software or programs.

27.15.22.7 The Contractor shall ensure that multiple logon sessions are not allowed in the System.

27.15.22.8 There shall be automatic logout after a certain period of user inactivity in a login session. The session time-out feature should be configurable.

27.15.22.9 Access controls shall be implemented in a fail-secure mode, which disallows access to the application system when authentication is not successfully completed.

27.15.22.10 Access to the system shall be controlled and granted on a need to basis. An access matrix and procedure shall be implemented to enforce this requirement.

27.15.22.11 The System shall allow the Authority and/or Engineer to control access to the published data for various access rights based on user-Ids and user groups.

27.15.22.12 All access to the application system shall be granted through the authentication mechanism.

27.15.22.13 The Contractor shall ensure that the strength of the authentication credentials commensurate with the risk of the System.

27.15.22.14 The Contractor shall implement account lockout when the maximum number of attempts is reached.

27.15.22.15 The System shall have the facility for deletion of the access rights of the users who have resigned from service in a timely basis to prevent unauthorized access.

27.15.22.16 The Contractor shall, at all times, leverage on a proven cryptography library implementation and not develop customized cryptographic libraries.

27.15.22.17 The Contractor shall ensure that the application system does not reveal to the users more information than needed when a failure or error occurs.

27.15.22.18 The Contractor shall implement Extended Validation (EV) digital certificate on the Internet-facing application systems.

27.15.22.19 The Contractor is responsible for tracking the expiry dates of all digital certificates and renew them before expiry.

27.15.23 Database Security

27.15.23.1 The Contractor shall propose a database with the necessary storage capacity (not shared with other customers of the Contractor) to house the Authority’s database and data.

27.15.23.2 The Contractor shall ensure that the confidentiality and integrity of the Authority’s data, files and information are preserved at all times. In

addition, the database shall also be secured against unauthorised accesses. The Contractor shall provide the necessary processes, procedures and mechanism to ensure that the violations of these requirements are made known to the Engineer within half-an-hour of their detection.

27.15.23.3 For data at rest, the Contractor shall ensure that commercially available encryption with no known vulnerabilities is deployed.

27.15.23.4 In the event of failure or disruption to database services due to the Contractor's actions, the Contractor shall be responsible for the recovery.

27.15.24 System Log

27.15.24.1 The Contractor shall review logs, including logs of activities carried out by privileged users, system/service accounts or administrator, regularly for security violation and security breaches.

27.15.24.2 The Contractor shall ensure that log information is accessed by authorised personnel only.

27.15.24.3 The Contractor shall ensure that logs are stored for at least one year to facilitate any incident investigation.

27.15.25 Audit Trail

27.15.25.1 All necessary and critical audit trail events, including system events, application events, business transactions and database transactions, shall be logged.

27.15.25.2 The audit trail reports shall minimally contain the following information:

a) Who logged in;

b) Where the connection was initiated from;

c) When the connection was made;

d) What was performed; and

e) Whether the action was successful or unsuccessful with error messages.

27.15.25.3 The audit trail shall be fully protected from any form of tampering, data loss and unwanted purging.

27.15.26 Security Assessment and Testing

27.15.26.1 The Contractor shall engage an independent party to conduct vulnerability scanning and penetration tests of the System by using industry proven tools before the System is commissioned. The reports shall be submitted to the Engineer for review. The Contractor shall be responsible for mitigating any security risks identified during the vulnerability scanning and penetration tests.

27.15.26.2 All security vulnerabilities identified by the IT security consultant shall be addressed by the Contractor to prevent exploitation of the System by potential external or internal threat sources. The Contractor shall propose and implement mitigating controls in the event that the security vulnerabilities cannot be resolved.

27.15.26.3 The Security testing is deemed complete only after the Engineer has accepted the security test plans and test results for the System.

27.15.26.4 The Contractor shall engage an independent party to conduct vulnerability scanning and penetration tests on an annual basis after the System is commissioned.

27.15.27 Security Audit

27.15.27.1 The Authority reserves the right to appoint a third-party auditor, Internal Audit or the Authority's IT Security team to audit the System for security compliance. The Contractor shall provide all support necessary for the conduct of the audit at no additional cost to the Authority. The third-party auditor's fees shall be borne by the Authority.

27.15.27.2 Should there be any non-compliance discovered during the third-party post audit, the Contractor shall also rectify the shortcomings within two (2) weeks from the date when the findings are reporting, at no extra cost to the Authority.

27.15.27.3 The Contractor shall provide evidence for the corrective and preventive follow-up actions to the Authority, no later than one (1) month after approval of the audit report.

27.15.28 Security Incident Response and Recovery

27.15.28.1 The Contractor shall develop incident response procedures in accordance with LTA IT Security Incident Management Process.

27.15.28.2 The Contractor shall report any observed or suspected security weaknesses or incidents immediately which may involve any loss, compromise or suspected compromise of classified information.

27.15.28.3 In the event of any security breach or security incident, the Contractor shall assist the Authority to:-

a) Investigate and analyse the cause or origin of the incident, and how it occurred;

b) Evaluate the extent of any damage;

c) Recommend methods or security controls to prevent the incident from occurring again; and

d) Provide full assistance to personnel from CERT, SingCERT, IMDA or law enforcement authorities in any investigation.

27.15.29 Cloud Requirements

27.15.29.1 The Contractor shall only subscribe to Cloud hosting services with a minimum Tier level 3 which have been independently audited or certified (such as Multi-Tier Cloud Security (MTCS) Singapore Standard 584) by competent third parties to be in compliance with industry Cloud security standards and be hosted in Singapore, subject to the Engineer’s acceptance. Information on the cloud hosting services and necessary certification shall be submitted as part of the proposal.

27.15.29.2 Any cloud related charges (e.g. data transfer, SMS charges) shall be deemed included in the Contract Price.

27.15.29.3 The Contractor shall be responsible for the management of the cloud services such as system administration, database administration, etc.

27.15.30 System Architecture

27.15.30.1 The Contractor shall implement the application system based on a multitier architecture. At a minimum, the database access tier shall be separated from other tiers if the application software is unable to support the multi-tier architecture.

27.15.30.2 The Contractor shall make sure that Web Application Firewall (WAF) is implemented to safeguard the Internet accessible application system against application-level attacks.

27.15.30.3 The Contractor shall propose UAT environment or servers to facilitate the development process and testing. All application enhancements

and patch management shall be tested on the UAT environment or servers before being deployed onto the Production environment.

27.15.30.4 The Contractor shall maintain the detailed logical diagrams and technical explanation of the system design, connectivity, architecture and functionality, including all interfaces with external parties.

27.15.31 Security measures for Cloud services

27.15.31.1 The Contractor shall ensure the following security measures are implemented when subscribing to Cloud services:

a) Security configurations are hardened and should be referenced to industry benchmarks such as NIST 800-53, Centre for Internet Security (CIS), or hardening standards provided by the product principal;

b) All logs are stored at secured locations to protect the integrity and ensure availability of the logs;

c) Application input fields are validated and failures are logged;

d) Firewalls or equivalent are implemented to protect the network against unauthorised traffic;

e) Intrusion prevention systems or equivalent are implemented to monitor the network or systems for suspicious activities to and from the Internet;

f) Administration to systems or applications is performed from an approved jump host or hardened device;

g) Vulnerability management processes are in place to identify and manage vulnerabilities, and security patches are kept up to date;

h) Vulnerability scanning and penetration testing are conducted; and

i) Suitable preventive controls are in place against malicious codes and malware (can include one or more of the following examples: restricting account privileges and use of administrative tools, application and process isolation, application whitelisting, secure web gateways, anti-malware software, and refreshes of approved Operating System image for stateless systems at least once a week).

27.15.31.2 The Contractor shall implement the below measures for remote administration to servers or applications:

a) Remote administration shall only be granted to authorised personnel;

b) Use 2FA to authenticate to the servers or applications; and

c) Logging of the date time, IP address, user information shall be enabled on the servers that allow remote administrative access.

27.15.31.3 The Contractor shall implement security patches in accordance with the below timeline:

a) Emergency patch – 24 hours deployment upon availability of patch;

b) High patch – One (1) month deployment upon availability of patch; and

c) Medium/Low patch – Two (2) months deployment upon availability of patch.

27.15.32 Security Monitoring and Incident Management

27.15.32.1 The Contractor shall ensure security related events are monitored for timely detection of suspicious activities.

27.15.32.2 The Contractor shall ensure security-related logs are available to facilitate event reconstruction and incident investigation.

27.15.32.3 The Contractor shall report all security incidents to the Engineer and work with the Authority in accordance with the Authority's IT Security Incident Management Process.

27.15.33 Cloud Asset Inventory

27.15.33.1 The Contractor shall be responsible for maintaining an asset inventory for all Cloud subscribed services, including software and tools deployed in the Cloud. The Contractor shall update the inventory at least annually and ensure tools and software that are not end-of-life (EOL) are deployed.

27.15.34 Safeguards for Personal Information

27.15.34.1 The Contractor shall implement safeguards in the System to protect sensitive data such as personal data in compliance with Personal Data Protection Act (PDPA).

27.15.34.2 The Contractor shall ensure that all user access to personal data are logged.

27.15.34.3 The Contractor shall ensure that personal data is encrypted at the database layer.

27.15.34.4 For database encryption and traffic tunnels encryption, the Contractor shall use commercially available encryption with no known vulnerabilities.

27.15.34.5 The Contractor shall implement measures to ensure that personal data fields such as NRIC and Passport numbers are being masked out when retrieved or displayed at the web pages/screens.

27.15.34.6 The Contractor shall ensure the principle of least privilege is adhered to.

27.15.35 Management of External Parties

27.15.35.1 The Contractor shall disclose details of key sub-contractors involved in the delivery of the work, including collection, usage or disclosure of data and be held responsible for all contractual obligations, including that of its subcontractors

27.16 General Operations & Maintenance Requirements

27.16.1 The Contractor shall submit the System Maintenance Plan to the Engineer for review and approval within one (1) calendar month before the Commissioning Date. This plan shall be updated periodically or when there are changes to the support information.

27.16.2 The Contractor shall be responsible for the following :-

a) Network and infrastructure maintenance;

b) Application maintenance Support;

c) Application operations and administration;

d) Database maintenance and support;

e) System monitoring and performance tuning;

f) Security management;

g) Backup and recovery management;

h) Contractor support structure;

i) Change Management;

j) System availability; and

k) System enhancement.

27.16.3 The Contractor shall ensure availability of necessary technical and maintenance support by the equipment specialist and the availability of the spare parts for the System throughout the System operation and maintenance period.

27.16.4 The Contractor shall submit his planned maintenance schedule detailing the checklist and frequency of the maintenance activities for the respective system equipment / components during the System operation and maintenance period.

27.16.5 All equipment shall be maintained in accordance with the manufacturer's recommendation. The Contractor is to provide manufacturer's recommendation in the System Maintenance Plan.

27.16.6 The Contractor shall recommend the maintenance regime or the parts required to be replaced during the operation and maintenance period. In the event that the replacement parts required are out of production, the Contractor shall submit the proposed new replacement part together with a compatibility test report to the Engineer for acceptance.

27.16.7 The Contractor shall ensure that hardware and software components are upgraded before it reaches end-of-support (EOS) or end-of-life (EOL).

27.16.8 The Contractor shall provide onsite support for the operations and maintenance services.

27.16.9 All work done on the System for installation, diagnosis or repair purpose shall be done with no or minimum disruption to the users' operations. In the event that an interruption is unavoidable, the Contractor shall propose an interim measure to capture manpower data during the period of disruption and the Contractor shall seek the Engineer's consent before proceeding.

27.16.10 The Contractor shall maintain an updated inventory list of all components of the System, including system documentation, cloud

resources, hardware, software, licenses and versions used by System at all the times. The inventory list shall be accessible by the Engineer at any time. A report summarizing the updated list of all components of the System shall be submitted to the Engineer annually.

27.16.11 The Contractor shall respond (within 2 hours) upon activated and shall resolve any faults within 5 hours of the occurrence of the fault. The Contractor shall provide all necessary hot standby spare parts to minimize the down time.

27.16.12 The Contractor shall be responsible to investigate the cause of any system defect or malfunction; and upon the completion of the investigation, submit a copy of the investigation report to the Engineer.

27.16.13 The System is considered to be defective if it suffers a loss of partial or full functionality for the intended purpose of this Contract.

27.16.14 The Contractor shall be required to repair / replace the defective system no later than three (3) working days from the time that the Contractor is informed that the system is defective.

27.16.15 In the event that there are major hardware defects affecting the reliability, availability and performance of the final production, the Contractor shall bear all incidental costs to carry out the replacement of the defective hardware without affecting the operation.

27.16.16 The Contractor shall provide trained personnel to do preventive maintenance and servicing of the System on a periodic basis (frequency to be approved by the Engineer).

27.17 Network and Infrastructure Maintenance

27.17.1 The Contractor shall proactively monitor the health of the network and infrastructure, ensure preventive maintenance is promptly carried out and initiate and co-ordinate all efforts required to upkeep the availability and performance of the network and infrastructure.

27.17.2 The Contractor shall perform the following network and infrastructure maintenance tasks:-

a) Configuration and installation of network services;

b) Co-ordinate with the telecommunications service provider for installation or fault diagnosis of communication lines;

c) Provide support and work with other teams to assist with problem isolation and resolution;

d) Restore network services in the eventuality of failures;

e) Administer, maintain, provide technical support and resolve problems for the network connectivity;

f) Monitor network performance and perform basic tuning to maintain performance; and

g) Disable unused services.

27.18 Application Maintenance Support

27.18.1 The Contractor shall provide the following maintenance and support services:-

a) Troubleshooting and resolution of production problems in the application software affecting the smooth functioning of the System;

b) Installation of application and any related software required for the smooth running of the application for users;

c) Delivery of all future updates to the application software and documentation to the Engineer;

d) Ensure smooth running of all components of the application software;

e) Provide corrective maintenance, trouble-shoot and isolate software defects, including diagnosis and correction of all latent errors on the application software;

f) Monitor application software to ensure data integrity and efficient performance;

g) Make presentations or conduct briefing of the application software when requested;

h) Produce updated technical and user documentation for the application software;

i) Proactively identify and recommend improvement areas to ensure continued operational efficiency of the System; and

j) Track and conduct details analysis of production problems trends / patterns such as program bug, aging, user group and etc. submit the continuous improvement plan.

27.18.2 In the case of future releases of application software offered, the Contractor shall keep the Engineer informed in writing and make available these new releases, licenses, and the relevant manuals after they have been released for general distribution.

27.19 Application Operations and Administration

27.19.1 The Contractor shall provide application operation and administration which shall include the following:

a) Prepare and perform the deployment process for bug fixes, implementation of application enhancements and development;

b) Participate and provide assistance in the user access control review exercise;

c) Produce and update technical and user documentation for the application;

d) Provide configuration, functional consultancy and technical advice pertaining to problem resolution or queries;

e) Provide technical advice and assistance to ensure the continuity, availability, and accessibility of the application; and

f) Implement and enhance operational procedures when needed.

27.19.2 The Contractor shall establish standard operating procedures to make sure that the account and access rights of user and external parties are updated in a timely way. The frequency of the review shall be:

a) All accounts – Annually;

b) List of inactive/suspended accounts – Monthly; and

c) List of staff who have left, redeployed or changed job role – Monthly.

27.19.3 The Contractor shall be responsible for the day-to-day administration, System monitoring and system health checks.

27.19.4 The Contractor shall advise the Engineer on the improvements to the availability and performance of the applications including middleware.

The cost of these improvements is deemed to be already included in the Contract Sum.

27.19.5 The Contractor shall analyse and track the performance bottlenecks, unresolved faults and provide rectification efforts to prevent the problem from recurring.

27.19.6 The Contractor shall propose and implement preventive action or improvement upon Engineer's acceptance. During the review meetings, the Engineer will analyse the progress of the fault resolution and prioritise the rectification effort.

27.19.7 The Contractor shall maintain and ensure all documentation is updated at all times to incorporate changes made to the application.

27.20 Database Maintenance and Support

27.20.1 The Contractor shall be responsible for the day-to-day backend database administration, management, operations and deployments.

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

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

27.20.4 The Contractor shall continually implement measures to improve the database availability and optimise database performance. This shall include, but not limited, to the following:

a) Constant and proactive monitoring and analysis of the system's resource usage, database utilisation, activities, performance and growth;

b) Perform database reorganisations and expansion;

c) Capacity planning; and

d) Identify resource intensive SQL statements, make recommendations to improve the efficiency of the SQL operations and implement the performance recommendations if required by the Authority.

27.20.5 The Contractor shall be responsible for database deployment activities which include database object & script deployment, script execution, etc.

27.21 System Monitoring and Performance Tuning

27.21.1 The Contractor shall proactively monitor the System which includes but not limited to servers, network and application systems for resource utilisation, faults, intrusions, security incidents, failures and System performance.

27.21.2 The Contractor shall provide System performance and fault monitoring services which include:-

a) Availability and status of critical processes or services;

b) Detect unresponsive critical processes or services (e.g. hung state);

c) Metrics reported by OS such as CPU, memory, swap space, disk, network and processes utilisation;

d) Monitored metrics which exceed the warning and critical conditions;

e) Overall health of virtualisation layers; and

f) Scheduled Jobs status.

27.21.3 The Contractor shall detect occurrence of any performance degradation and fault of the services and systems and take immediate actions to ensure that the Authority's defined service levels are met.

27.22 Security Management

27.22.1 General Requirements

27.22.1.1 The Contractor shall have security processes in place that minimally covers the following:-

a) Processes for monitoring activities of personnel with system, database or network super user and/or administration rights. The Contractor shall have an internal process to monitor and review activities and audit trails of their personnel who have 'root' or system administration privileges;

b) Processes for reviewing accounts (including redundant / suspended / test accounts) and ensuring these are removed in a timely manner. Where possible, accounts shall be revoked / removed on the last day of the service. Accounts shall be reviewed periodically;

c) Processes for review of the System's logs and audit trails;

d) Processes for obtaining, evaluating and applying security patches;

e) Processes for transfer of duties from personnel to personnel;

f) Practices for ensuring segregation of roles and responsibilities;

g) Processes for pre-emptive checks on the System which shall include putting in place a calendar on the checks to be performed based on past common audit findings and gaps identified from various reviews such as vulnerability assessments and security compliance review;

h) Processes for subscribing, evaluating and acting on vulnerability alerts / security advisories The Contractor shall implement measures (for example, security patches and operating system hardening) to address security alerts and security gaps;

i) Processes for monitoring, detecting, responding, and managing security incidents; and

j) Processes for system backup and restoration.

27.22.1.2 The Contractor shall maintain a list of all patches / security fixes / updates applied to the operating environments, security patches applied, audit trails and security-related log review, virus detected, etc. as part of the Progress Report.

27.22.1.3 The Contractor shall ensure that its personnel are sufficiently trained in IT security and are aware of the security considerations and implications of the works performed.

27.22.2 System Security

27.22.2.1 The Contractor shall assist in the management and configuration of firewalls and other security services supplied as part of the contract. This shall include the administration and maintenance, problem resolution and technical support, performance and fault management and account management.

27.22.2.2 The Contractor shall provide security administration for the systems and servers.

27.22.2.3 The Contractor shall ensure that there is no sharing of accounts and passwords. The Contractor shall maintain an account access matrix and authorised account list for each sub-systems.

27.22.2.4 The Contractor shall review and monitor user accounts, security access logs, audit logs, system logs, event logs, security logs, file changes, etc., and alert the Engineer on any abnormal activities, exceptions or suspected intrusion. All logs shall be stored for review (to detect a pattern, if any) for a minimum period of three years.

27.22.2.5 The Contractor shall keep the System free of malware and viruses. The Contractor shall update all anti-virus data files on all systems used in the operating environment within TWENTY-FOUR (24) hours upon release by the Anti-Virus vendor. The Contractor shall put in place automatic anti-virus software and / or virus data file update process on all servers. In the event a virus is found in the System, the Contractor shall inform the Engineer and advise the Engineer accordingly of the impact and its remedy action.

27.22.3 Security Patch Management

27.22.3.1 The Contractor shall evaluate and test all latest security fixes / patches updates and apply the necessary patches or upgrades onto the affected software of the System.

27.22.3.2 In the event a security fix cannot be applied, the Contractor shall inform the Engineer and advise the Engineer accordingly of the impact.

27.22.4 Security Monitoring and Response

27.22.4.1 The security monitoring mechanism shall have monitoring and alerting features that can alert the system administrator within given time frame based on incident response procedures developed.

27.22.4.2 The Contractor shall detect and investigate security breaches and report them to the Engineer immediately.

27.22.5 Security Vulnerability Management

27.22.5.1 The Contractor shall conduct annual vulnerability assessment/scanning and penetration testing and ensure all follow-up actions identified during the assessments are duly addressed.

27.23 Backup and Recovery Management

27.23.1 The Contractor shall provide comprehensive System backup and recovery management services.

27.23.2 The scope of the System backup and recovery management services shall include the proposed platforms, applications, programs and databases.

27.23.3 The Contractor shall perform periodic checks on the status of System backup jobs to ensure successful completion of scheduled Server backup jobs and the actual backup.

27.23.4 The Contractor shall verify and record the results of every server backup job and schedule to re-run any incomplete / unsuccessful backups whenever possible.

27.23.5 The Contractor shall maintain System backup configurations / specifications and recovery procedures to ensure that they are always up-to-date, correct and effective for data recovery at all times.

27.23.6 The Contractor shall test and verify all new server backup configuration / specification and recovery procedure prior to deployment.

27.23.7 The Contractor shall perform server data recovery based on the Server backup and recovery procedures.

27.23.8 The Contractor shall perform restoration and archive requests for data / file / folder / system / database.

27.24 Contractor Support Structure

27.24.1 The Contractor shall describe fully the support structure in place to deliver 24/7 support and services to the Authority.

27.24.2 The Contractor shall ensure that the support personnel are trained to carry out the services, and appropriate back-up personnel are available whenever necessary to support the operations.

27.24.3 The following local support structure shall be available:-

a) Product specialists trained in the support of the product;

b) Local support centre for helpdesk service;

c) Technical support for problem determination and resolution; and

d) On-site support.

27.24.4 The Contractor shall be solely accountable for the Operations and Maintenance Services.

27.24.5 Phone Support

27.24.5.1 Phone support via helpdesk service shall be available 24/7 from the Contractor for all problems reporting. To ensure quick response from the Contractor, it is expected that the relevant Contractor's personnel shall carry hand-phones whose numbers shall be made available to the Engineer. Phone facility shall be available from the Contractor for all problems reporting.

27.24.6 Service Escalation List and Mechanism

27.24.6.1 The Contractor shall provide a service escalation list of personnel to contact in the event of problem escalation or service rendered.

27.24.6.2 The Contractor shall provide a list of support personnel and their respective areas of expertise. This list shall be updated whenever there are changes. The Contractor shall provide an escalation mechanism to reach the support and alternative personnel.

27.24.6.3 There shall be clear indication of the problem escalation structure within the support structure. The Contractor shall provide the problem escalation / resolution support team structure.

27.24.7 Incident / Problem Management

27.24.7.1 The Contractor shall capture, monitor and report all defects, conduct analysis, resolutions up to problem closure. When requested the Authority's appointed staff shall have full access rights to all information captured.

27.24.7.2 The Contractor shall provide problem diagnosis, resolution and incident management for the System by co-ordinating the entire effort.

27.24.7.3 The Contractor shall provide second level support via Helpdesk Service when any part of the System is down which includes leading the problem determination and resolution, supervision and liaison with the relevant parties / vendors till the problem is resolved.

27.24.7.4 The Contractor shall assist the Authority, in the event of general performance degradation of the System by utilising specialised devices

or scripts as requested and authorised by the Authority, to collect, analyse and interpret the collected data as well as recommend the necessary follow-up activities to resolve bottlenecks or congestion within the System.

27.24.7.5 The Contractor shall remove all bypass solutions once the problem is resolved.

27.24.7.6 The Contractor shall be required to attend ad-hoc meetings when necessary during the problem resolution and incident management phases.

27.24.8 Monthly Summary Reports

27.24.8.1 The Contractor shall propose the monthly report formats for the Engineer's approval. The Engineer may review and make any amendments to the report formats from time to time.

27.24.8.2 The monthly reports shall cover the following:-

a) Performance of Service Levels;

b) Report on System availability;

c) Collated incident and problem Logs;

d) Resource Utilisation;

e) User account and access right review;

f) Log review; and

g) Any other details requested by the Engineer.

27.24.8.3 The Contractor shall produce ad-hoc progress report when requested by the Engineer.

27.25 Change Management

27.25.1 The Contractor shall document all changes and ensure that proper change management procedure is in place for tracking and managing changes to software and systems. This shall include the following:-

a) Impact analysis shall be carried out prior to the change so as to minimise impact due to the change;

b) All changes to the production systems shall be formally authorised and documented; and

c) All items being rolled out or changed are secure and traceable, subjected to the approval of the Engineer.

27.26 System Availability

27.26.1 General requirements

27.26.1.1 The total operating hours of the System is deemed to be 24 hours a day, 7 days a week and 365 days a year throughout the contract period.

27.26.2 Availability requirements

27.26.2.1 The System shall meet the availability requirements as shown in the table below:

Availability Requirements

Measurement	Availability Requirements
System uptime per calendar month	99%

27.26.2.2 The System shall meet the availability level requirements starting from the Commissioning Date.

27.26.2.3 System Availability Level shall be determined according to the following formula:

System Availability = [Operational Hours – System Downtime] / [Operating Hours] x 100%

"System Downtime" means the accumulated time during which the System is not performing due to product failure measured from the time the Contractor is informed by phone of the product failure to the time when the System is returned to proper operation

27.26.2.4 The Contactor shall provide a detailed calculation for the System Availability in terms of percentage.

27.26.2.5 The System shall be considered inoperable, partially inoperable, or unavailable under any of the following conditions:-

a) Any of the servers becomes inaccessible;

b) Any of the services on any of the servers becomes inaccessible (e.g. database service becomes inaccessible on the System Production Server);

c) Any of the services on any of the servers does not respond properly;

d) Any of the applications on any of the servers becomes inaccessible; and

e) Any of the System interfaces to the external systems does not function.

27.26.2.6 The Contractor shall propose the scheduled downtime and frequency for maintenance activities for optimum system performance and efficiency. This is subject to approval by the Engineer.

27.27 System Enhancement

27.27.1 The Contractor shall provide services for modifications and enhancements to the System, as required by the Authority.

27.27.2 The Contractor shall track, capture, manage and report the status of the enhancements.

27.27.3 The Contractor shall carry out the following: -

a) submit a detailed proposal or Impact Analysis to the Engineer according to the nature of work;

b) include a breakdown of the man-day effort sizing for the works to be performed and quote the cost for the works using only the items and their corresponding rates quoted in the Schedule of Rates; and

c) provide justification of the sizing.

27.27.4 The Contractor shall submit and update the following documentation as part of the deliverables:-

a) Requirement Specification;

b) Technical Design Specification; and

c) Test plan and test result.

27.27.5 This system enhancement shall be paid based on the man-day rates priced in the Schedule of Rates.

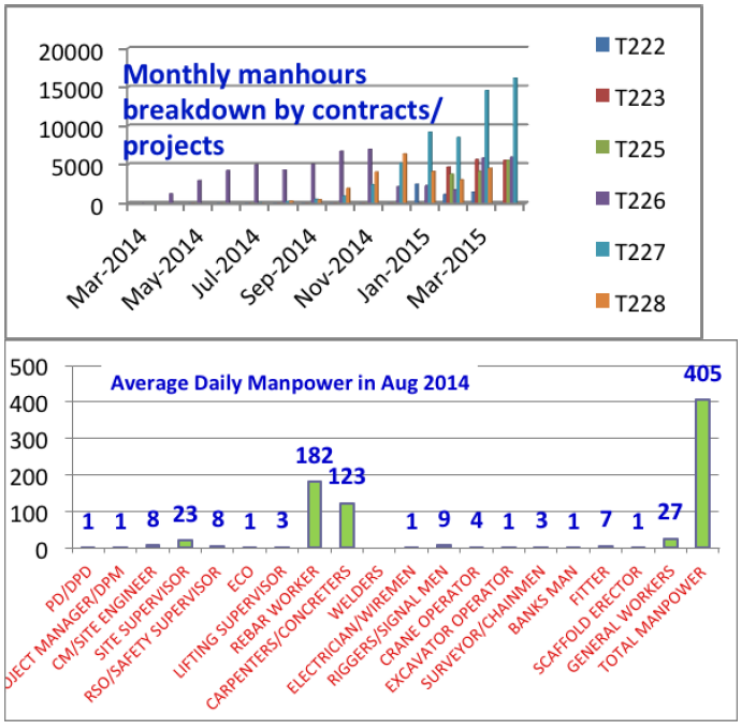
27.27.6 The Contractor shall not commence any works without the approval of the Engineer.

Appendix PS-27-A Example of User System Access Rights

Account		Access Rights :						
Admin Staff	Project Staff	Create account for Admin Staff and Project Staff	View Contract CR206	Submit data & project information	Amend data & project information	Upload monthly manpower report (ePSS)	Download Manpower/P(S) daily/weekly/monthly reports	Download other Management Reports
LTA Master Admin	LTA HQ	√	√	√	√	√	√	√
LTA CR206 Admin	LTA CR206 Team	√	√	√	√	√	√	
The Contractor Admin	The Contractor for CR206 only	√	√	√	With approval from LTA CR206 Admin	√	√	
QP(S) Admin	QP(S) for CR206 only	√	√	√	With approval from LTA CR206 Admin		√	

Note : Actual user system access rights to be agreed with Authority after tender award

Appendix PS-27-B Examples of Output Screen Display/Report



Sample screen display or printout on manpower to be available in system for:

- Project
- Contract

System should allow generation of graphs, depending on selection by user

E.g.

Monthly man-hours breakdown

Average daily manpower by trades per month

From start of RC works progressively up to completion of Basic Structural Completion

Trade Productivity for RC Works				
Item	Quantity Completed	Total Mandays Utilised	Productivity Rate	Remarks
Concrete Placement				M3/manday
Reinforcement Fixing				Kg/manday
Formwork				M2/manday

Sample screen display or printout on Productivity Performance on Contractor to be available in system for :

- Project
- Contract