Scope of Panchdeep O & M for DC and DRC

The Data Centre is located at ESIC Hospital premises Rohini, New Delhi and the Disaster Recovery Centre is located at Hyderabad, Telangana. DR environment is similar to DC environment and shall be maintained in a similar manner.

24*7 Services shall be provided for Operations & Maintenance Support of existing Panchdeep Applications, Infrastructure, Hardware, Network Management System and Building Management System as per Service Levels defined in RFP.

1. Operations and Maintenance of DC & DR

a) All existing IT processing facilities and BMS assets at DC and DRC shall be maintained by new Service provider. Defective asset, out of support asset from OEM if any, shall be reported to ESIC during takeover from existing service provider. For Asset details please refer annexure 01 and 02.
b) Service Provider shall provide Maintenance of Building Management System consisting of IT related power (excluding raw power), cooling, earthing, UPS, Genset, PACS, Air Conditioning, Access cards, CCTV camera, Fire suppression, Fire protection, rodent repellent at DC and DRC. Maintenance includes upgrade/update/replacement including defective part replacement; patch and version update during the entire period of the contract. Service Provider shall plan for alternate power backup of minimum 08 hours. Service provider shall provision for diesel generator fuel accordingly.
c) The Service Provider shall maintain all existing ESIC applications available on Internet and intranet.
d) Service Provider will conduct Preventive Maintenance activity in every quarter which includes rack dressing, DC/DRC systems health check-up, IT room devices basic hygiene check. Service Provider is responsible for Rack numbering, cable dressing and Labelling. Service provider to submit the report with artefacts.

Physical Security

e) The existing physical security perimeter for hosting the project infrastructure in the DC and DRC should be maintained.
f) Unauthorized person shall not be allowed beyond existing isolated Physical Access points located inside DC and DRC without ESIC permission.
g) Service provider shall maintain existing Access control mechanism in DC and DRC located at different areas. Existing Biometric Access attempts successful or failed should be logged.
h) Each visitor must be provided with an ID card and shall always be accompanied by a staff within the premises. Visitors shall not be given access for computer room (information processing facilities inside DC and DRC) unless approved by appropriate authorities

i) All employees/staff working at data center shall be provided with a photo identity card with appropriate physical access as per their roles and responsibilities
j) Media (Disk, Tape) shall be disposed of securely when no longer required using formal procedures. All faulty non serviceable asset except replacement equipment's from OEM and hardware service and support provider shall not be returned to service provider
k) The Data Centre building must be monitored through CCTV Surveillance round the clock.
l) The CCTV cameras are installed around the perimeter of the building, entrance and entry points and critical points within the building. The Vendor has to maintain them and recordings of the CCTV Camera shall be stored for a period of 6 months.
m) Access to Video recordings should be allowed only to authorized personnel from ESIC.

Backup

n) Service Provider shall operate and maintain existing backup and recovery assets at DC and DRC.
o) Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy

Security and Compliance

p) The DC and DRC Application, Infrastructure and Network shall be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification using existing tools and countermeasures at DC and DRC.
q) Service Provider shall adhere to all ISMS policies laid down by ESIC and ISO 27001 latest standards.
r) The existing Security measures and tools deployed at DC and DRC shall be monitored via automated tools in DC and DRC
s) Patch and version update of all the existing infrastructure devices, Network devices, Infrastructure applications and tools shall be carried out during the entire period of the contract. Patch update shall include bug fixes, Firmware, software maintenance release provided by OEM.
t) Service Provider shall provide hardening of network, infrastructure and applications using existing tools.
u) Service provider shall provide antivirus and anti-malware management using existing tools
v) Service provider is responsible for maintaining Infrastructure, Network and application license compliance at DC and DRC for the entire period of the contract. The license ownership documents of all assets shall be provided to ESIC or its agency.
w) Service Provider is required to make all USB removable storage read-only and Disable all CD/DVD burners, except ESIC authorized devices.

NOC and SOC Operations

x) Service provider to operate existing NOC and SOC in DC. Service provider to adjust NOC and SOC configuration using existing tools and countermeasures to cover the ever changing threat landscape as per ESIC requirements and SLAs, as and when required.

VoIP and VC

y) Service provider shall maintain existing Centralised unit in DC and DR of VOIP and VC .VOIP services are existing for 15000 phones and VC services support 225 Video conferencing endpoints at various ESIC locations.

2. Operation and maintenance of Applications

a) The Service Provider will ensure that source code of existing applications should be securely maintained in ESIC DC and DRC. All source code check-in check-out, build, release and deployment happen from the ESIC information processing facilities at DC and DRC only. Admin and Super Admin access of source code repository remains with ESIC and ESIC appointed agency only. Relevant check-in/checkout permission will be given to the application team as per requirement.
b) The Service Provider shall provide routine functional changes that include user and access management, user registration, deregistration of new roles, configuration of reports, and addition of new roles for accessing existing services.
c) Service provider shall provide reports as required by ESIC. It includes generation of adhoc reports, new reports and modification of existing reports in MIS and BI application.
The Service Provider will ensure that development of the application must be done using secure coding best practices and standards. Post the functional UAT approval, the application should be validated by application security team. Service Provider shall provide artefacts to ESIC or ESIC nominated agency for verification of secure coding best practices followed by them.
d) Any changes to the application suite during the Operations and Maintenance Phase will be released to production only after successful regression testing, load testing, stress testing including automated testing where necessary, of the application. The regression, load, stress test plans shall be provided in advance to the ESIC for approval. Application Testing shall be automated to reduce the manual error and testing effort.
e) Provide Release Management and Deployment plan for planned release and deployment of the application change or upgrade of application.
f) Service Provider shall tune application, databases, third party software's , automation of processes, batch process creation, job creation, scheduling and any other components provided as part of the solution on routine basis to optimize the performance.

3. ESIC User Trainings

a) Service Provider shall provide hands on user training on Existing Panchdeep application users as per the mutually agreed schedule between ESIC and Service Provider.
b) The schedule for classroom / instructor-led training to end-users will be jointly prepared by ESIC and the Service Provider. These trainings will be conducted at various ESIC offices. Travel and stay arrangements will be provided by Service Provider. It is expected that 6 dedicated trainers will be made available by Service Provider for conducting these user trainings.
c) Service Provider should update and maintain the existing necessary manuals and training materials (including Training materials / user manuals) for all the module and applications. These manuals should be updated as and when features / functionalities in the system changes with auditing and audit trail. The manuals are hosted on the portal and available to the users. No separate Print out cost shall be provided to service provider.

4. Service Desk

a) The service will be provided in English and Hindi. The service should be available 365*24*7 to the users
b) The service will serve as a single point of contact for reporting and resolution of all tickets (queries, errors, incidents, issues). These tickets may relate to any business or IT operations of Panchdeep
c) The service will also serve as a single point of contact for reporting of all MPLS/Internet/SDWAN queries and issues. Service desk will be required to forward the calls to respective service provider and follow-up.
d) The Service provider shall maintain existing Service Desk and its tools at DC with minimum of 15 (This is an Indicative figure, Service Provider is required to gear up for its load) hunting lines of VOIP with Interactive Voice Response (IVR) System, for first level of call segregation, with call recording facility. The Service Desk is to be manned by at least 16 resources in general shift and 20% of that in other shifts to attend the call volumes. The Service Provider shall gradually increase the number of hunting lines and resources to meet the 10 % annual growth in call volumes.
   Service provider shall pay for all the telephone rental and facilities.
e) Activities under the responsibility of the Service Desk include:
   i. Assign severity level to each ticket as per the SOPs. Track each ticket to resolution
   ii. End user support in case of technical difficulties in use of the software, answering procedural questions, email related queries, providing recovery and backup information, and any other requirement that may be incidental/ancillary to the complete usage of the application
   iii. Provide the first level of support and routing the query received to the concerned team of the Service Provider for resolution of tickets that are beyond the scope of Service Desk team
   iv. Escalate the issues / complaints, to ESIC if necessary as per the escalation matrix.

v. Notifying users of problem status and resolution through the tickets over email / SMS where available. Service provider shall provide SMS gateway and application at both DC and DR. SMS cost shall be paid on actual after the end of each month to Service provider

vi. Regular Monitoring of tickets and daily, weekly and monthly dashboards to be shared with ESIC

vii. Prepare Knowledge base for frequently reported problems along with the resolution steps / solutions and publish on the appropriate portal, front office or back office for the users. Publish and continuously update the knowledge basis on the website that can enable end-user to find resolution without calling the Service Desk.

viii. On a quarterly basis, Service Provider shall carry out the analysis of help desk tickets (open and closed) and field assessment reports provided by ESIC or its monitoring agency to identify the recurring incidents and conduct a root cause analysis on the same. Service Provider shall submit a report to ESIC with the analysis and provide inputs to ESIC on End User training requirements, awareness messages to be posted on the portal, redesign recommendations and / or application enhancements (functional / design) based on help desk ticket analysis. The objective of the analysis should be to address the repeat incidents and enhance the delivery of services to the end users, front office as well as back office users. (ESIC location Assessment is carried out by monitoring agency of ESIC)

ix. Periodic Review of service desk Standard Operating Procedures with call prioritization guidelines, problem severity codes, and escalation procedures in consultation with ESIC

5. Project Management Artifacts for Operation and Maintenance and Change Request

Service provider is expected to provide following Project Management Artefacts for Operation and Maintenance and Change Requests

a) Project Management Plan including:

- Release Management Plan
- Software Quality Management Plan
- Quality metrics
- Quality checklists
- Communication Management Plan
- Risk Management Plan
- Process Improvement Plan
- Incident Management Plan
- Database Backup & Recovery Plan
- Software Configuration Management Plan
- Change Management Plan
- Configuration Management Data Base (CMDB)
- Release Notes (Document mentioning deployment details of components, build, timestamp, rollback plan, smoke testing, etc.)

b) Issue Log (list of ongoing and closed issues of the project)
c) Change Request register (repository for all changes requested with details for ongoing and closed Change Requests)
d) Service provider shall maintain a document of Knowledge Based Information Document (KBID), Trouble Shooting Resolution Learnings.
e) Service Provider shall keep all project documents up-to-date with existing version control mechanism during the course of the project.