APPLICATION FOR CO-HOSTING IN STATE DATA CENTRE
&
SERVICE LEVEL AGREEMENT

Name and Address ofthe Department/Organization	
Office phone number	
Official e-mail id	
Name and Contact number of Administrative Head	

Technical Team

	Name, Designation and Organization	MobileNumber	Office Phone Number	Official e-mail id
System Administrator				
Development Technical Lead				

*The above contact details will be used in emergency situation when service is affected

Web Application Details

Domain Name	
Brief Description about application	
Programming Language used and Version	
Any Content Management Framework used and version	
Any Coding Frameworks used(e.g, Codeigniter, Java	

Spring, Silverlight)	
Database(with version)	
Any other technologies used	

Any third party components (including CMF components)/ plug-ins/libraries used:

Library Name	Version	Functionality and Publisher of library

Any external dependencies used (web services/ payment gateway services/ email etc):

External Application	End point	Technical details of the external application

<u>Application services available</u>:

Pleaseselect the requiredservices

1. Linux / Apache / PHP/ JBOSS:...
2. Windows / IIS /ASP:...

By default we provision 250 MB application space. If extra space required we can provide up-to 5 GB maximum.

Application Space Quota Required in (MB/GB):..

<u>DatabaseServices:</u>

Note: Database access will only be given from the application server and the database cannot be accessed directly from Internet.

Available Databases in SDC:

1. MS-SQL: ClusteredDatabase.
2. MySQL: With replication.
3. Postgres SQL: Withreplication.

a) Required DatabaseName:...

b) Space required for database in (GB /TB):...

Platform as Service: OS platform available to host theapplication:

1. Linux(RHEL):...
2. Windows : ....

Remote access:

- Local/Remote Access required: YES / NO

➢ If Yes, Please update the belowdetails:

a) Static Private IP address: (KSWAN):..

b) Static Public IPaddress: …...

Application Ports:

Server	Protocol Type	Application Port Numbers to enable
App Server		

Additional Information

Estimated total number of concurrent customers	
Any peak time for the application (any particular time during the month/ year)	
Any Performance requirements of the application	
Any Constraints of application	
Criticality of application	□ Low

	□ Medium □ High
Reason for criticality	
Is Software Application Architecture Document submitted? (See Terms & Conditions No.1)	□ Yes □ No If No, specify date by which it can be emailed to cert.ksitm@kerala.gov.in and to respective SDC's email id's alsosdc1.ksitm@kerala.gov.insdc2.ksitm@kerala.gov.in.: …./…./……

Terms & Conditions for Co-Hosting

1. The department shall maintain technical documentation including Software Application Architecture document. The Architecture document should include application details such as Application Overview and functionalities, Component architecture diagram showing inter dependencies and any external dependencies, technologies used, deployment architecture, deployment configurations, revision history of document etc. Updates to the document should be versioned as separate versions and maintained. The architecture document shall be shared in print along with the hosting request form or mailed to cert.ksitm@kerala.gov.inand to respective SDC's email id's alsosdc1.ksitm@kerala.gov.in, sdc2.ksitm@kerala.gov.in

2. The application will be hosted under Staging Server for a period of three months from the date of presenting the filled application form for conducting Security Audit. If the process is not completed in the 3 month period, the application will be deallocated from Staging Server without priorintimation.
3. Security auditing of the application by any CERT-IN empaneled agency or CERT-K has to be carried out in the hosting environment. A copy of the security certificate shall be provided to the SDC. The SDC should allow hosting on production servers only after receiving security audit certificates (safe to host certificate) which needs to be maintained in records.
4. Due to stringent security policy implemented in the server, some of the functionalitiesof the application may not work as expected.All functionalitiesof the web application should be validated in the staging server.
5. KSITM has set a maximum space limitation on Web / Application to 10 GB and DB Storage limitation to 2 TB for all Departments for Co-Hosting which can be increased uponusage.
6. Access to the Database server will only be given from the application server. The database server cannot be accessed directly fromInternet.
7. Application level security is solely under the privilege of the Department. It is the Department/authorized vendor's responsibility to tighten the security of the application. By the

above condition,it should be accepted that the Department shalltake thefollowing measures:

i. The environment is a shared one. The Department shall be committed to maintaining the security of its own applications. Security compromise arising from a single application could potentially result in adverseattacks on other applications hosted on the same server. Application Security needs to be a significant consideration during the development of any software. Additionally, security patches post production also needs to be factored into the contract with the application development vendor.

ii. Have maintenance contract such that technical support is available at any point of time to address any request for enhancement, upgrades, security remediation, migration and testing of the application.

   - Upgrades/ patches are frequently released by vendors/ open communities for any software (including Operating System, Database, Application Server, Programming technology such as Java, various code frameworks and commercial/ open source libraries and components) to address added functionalities as well as security vulnerabilities. It is the responsibility of the application support team of the department to proactively identify patches to any technologies/ components used in the application and apply these after proper testing.
   - The platform (OS/ DB/ Application Server) provided may also be upgraded by SDCwhenever significant patches for vulnerabilities are released. It is the responsibility of the department and its application support team to ensure that the application works correctly on the upgraded platform.

iii. Comply with Government Order G.O.(Ms) No.43/2015/ITD dt 01.10.2015:

   - Periodic security auditing is necessary. The department shall get the sites audited once every 2 years by a CERT-IN empaneled agency. If an application is developed in an agile manner such that enhancements to the application are rolled out frequently, the department is required to have Security Audits done by a CERT-In empaneled agency once every 6 months
   - Once audited and hosted, the department/ Technical Lead shall raise a Change Request (CR) and submit the CR form to SDC if any subsequent change is to be made on the application including any configuration change or patch application.Updated Software Application Architecture Document also needs to be submitted.The Change Advisory Board shall verify the technical changes and evaluate if a subsequent security audit is required before the changes are deployed on the production server.
   - If any change to the application is deployed without intimation to the SDC, Director, Kerala State IT Mission reserves the right to de-allocate domain name and pull down the web site.
   - Upon identification of any security compromise arising from the application, SDC/KSITM will have the complete right to block the application. In order to regain access to the application software, theDepartmentwillhaveto get theapplicationre-audited beforegoingonlineagain.
   - Director, Kerala State IT Mission is authorized to order de-allocation of the domain name and pull down Government web sites if security level of the site is found to be

insufficient at any point of time.

- The department is required to submit any application logs and dumps that are required by CERT-K for any analysis.
- Contents of the websites/applications shall not be against the interest and reputation of Government of Kerala.

iv. As part of application level security,it is mandatory that the Department ensures a strict password policy.

v. If any hacking occurs due to any vulnerability present in the application, the Department will be heldresponsible for compromising the security of the server.

8. The expense required for any technology upgrade for the purpose of hosting at SDC shall be met by the Department concerned.
9. Any change in Technical Representatives must be intimated to KSITM.
10. Prior approval of KSITM must be taken for any kind of planned activities like VA, PT of the application.

NOTWITHSTANDING, BY USING THE SERVICES, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND AGREE TO BE BOUND BY THE TERMS AND CONDITIONS CONTAINED HEREIN INCORPORATED BY REFERENCE.

SignatureofAdministrative
Head ofDepartment

Signatureofthe Approving Authority

Designation Seal

Office Seal

Signature of Technical Lead

Date: / /

Date: / /

SERVICE LEVEL AGREEMENT

This **SERVICE LEVEL AGREEMENT** (“Agreement”) made at Thiruvananthapuram on dd-mm-yyyy

BETWEEN

The Director, Kerala State Data Centre, (SDC-1, 4th Floor, Co-Bank Tower, Thiruvananthapuram,Kerala OR SDC-2, Thejaswini -1, Technopark, Thiruvananthapuram, Kerala). For and on behalf of Kerala State Information Technology Mission (KSITM), Vellayambalam, Thiruvananthapuram

AND

“Name **of the Dept**.” ……………………………………………………………………………….. and

having its office at ………………..………………………………………………………...Dept address

“………,

hereinafter referred to as “Subscriber”

WHEREAS

1. KSITM has established Kerala State Data Center in Co-Bank Tower &Technopark campus, Thiruvananthapuram for providing Managed Services on a non-exclusive basis within the geographical area specified.

2. The Subscriber, for its Network monitoring and management needs, is desirous of availing the Services of SDC for managing/monitoring its network as per the deliverables specified in the scope of services below for its offices across the defined geographical area.

3. SDC is agreeable to provide the Managed services to the Subscriber and the Subscriber is agreeable to avail the Managed Services from SDC on non-exclusive basis on the following terms and conditions.

NOW THIS AGREEMENT WITNESSETH AND THE PARTIES HERETO AGREE AS FOLLOWS:

1. **Term**: This Agreement shall be deemed to have commenced from the Date of Service commencement and shall remain in force initially for a period of three years. Unless this Agreement is terminated by the Parties in writing, the same shall stand automatically renewed for a further period of one (1) year on each occasion provided the Subscriber has made the payments due, if any, under this Agreement or any renewal thereof from time to time. Any amendment in the agreement can be done, if required, by only the authorized personnel at SDC and authorized personnel/IT Head at the subscriber’s end by mutual consent.

Signature   Signature

KSITM Director

2.**Scope of Service**: Subject to terms hereof and based on the representations, warranties and undertakings made by the Subscriber as contained in Clause 5, SDC agrees to provide the managed services to the Subscriber as per Agreement

3. **Terms and Conditions of Managed Services**: The Managed Services shall be provided by SDC to the Subscriber subject to the following terms and conditions under the mentioned Service Window. The Service Window is as specified.

PWH (Prime Working Hours): 8:00 AM to 8:00 PM (Monday to Saturday),

EWH (Extended Working Hours): 8:00 PM to 8:00 AM (Monday to Saturday), Sunday and all State Government Holidays excluding regional holidays.

Severity (Refer Annexure 1)	Response Time		Resolution Time	
	PWH	EWH	PWH	EWH
1	10 minutes	20 minutes	Within 60 min / 1 hour	Within 240 min / 4 hours
2	20 minutes	60 minutes	Within 240 min / 4 hours	Within 480 min / 8 hours
3	30 minutes	120 minutes	Within 480 min / 8 hours	Within 720 min / 12 hours

The resolution/Implementation time will exclude time taken by third party dependency in terms of Vendor support and will consider the exclusions mentioned. The vendor SLA commitments will be carried forward to the Subscriber. SDC will drive the respective vendor for the concerned issues and adhere to their agreed SLA for Co-Hosting services

4. **SDC Commitment and Exclusions**.

4a. SDC will be responsible for providing the Services as per the service catalogue (Annexure 3) Commitment: SDC shall be responsible for the provision of the following services.

- SDC Help desk will cover the first level call reporting. Subsequent SLA management will be the responsibility of the Subscriber

- SDC will provide internet access to the servers as required

----

Signature Signature

KSITM Director

- SDC shall provide network and physical security

- SSH access, if required, shall be provided on written request from the Subscriber, subject to technical feasibility

4b. Exclusions: SDC shall not be responsible for any Fault to the extent that such Fault results from any of the following events

- Any force majeure events and other causes beyond reasonable control of Kerala State Data Centre.
- Any interruptions resulting from defects or failures in or use of the Subscriber’s provided apparatus or equipment, Subscriber’s co-location equipment or any Services or any facilities provided or operated by or on behalf of the Subscriber

- Incomplete, misleading, inaccurate information provided by the Subscriber to SDC.

- Any delay or failure in complying / executing any of the Subscriber’s obligations for Services like Move, Add, Change, Delete (MACD) in any way at Subscriber’s request within a notice period as agreed by Subscriber &SDC.

- Any Planned Work which will be notified to the Subscriber well in advance through portal (http://itmapp.keralaitmission.org) Events or occurrences where the Subscriber logs Trouble Ticket but there are no faults been detected by DCO.

- Any act/omission on the part of the Subscriber including but not limited to failure to notify the Service desk.

- The failure of Subscriber’s applications, equipment or facilities including any third party equipment.

- Accident, neglect, misuse or default of the Subscriber, it’s employees or agents or any third party

- Trouble ticket associated with new installations of any modules into the present hardware by the subscriber without information of SDC.

- SDC will provide periodic report as agreed to the Subscriber for review.

- SDC shall be responsible for Site(s) being non-operational only if it is due to problems related to the equipment at Site(s) supplied by SDC.

---

Signature   Signature

KSITM Director

- The usage of helpdesk for Managed Services as indicated by the SDC will be 24*7.
- All license issues for Co-location services to be settled by Subscriber.

4c. Exclusions – Disaster Recovery (DR) services

- No DR service will be provided to Co-Location servers. However, subscriber will be allowed to use the existing connectivity to the National Data Centre, New Delhi, on need basis
- DR Services will be provided to Co-Hosted applications on need basis only at NDC, New Delhi, subject to availability of resources and approval from KSITM. DR services will be provided on request to co-hosted

5.**Representations, warranties and undertakings of the Subscriber**: The Subscriber represents warrants and undertakes to SDC that:

5.1. It shall follow and meet mandatory requirements of security audit and submission of "Safe to Host" certificate as mentioned in and issued by SDC. Server hardening need to get complete before go live of co-hosted or co-located application. The Subscriber has read and understood the mandatory business requirements and is aware that unless these requirements / instructions are met at all times, SDC will not and shall not be responsible for any non- availability/degradation in performance of the Managed Services.

5.2. To make payments to SDC in accordance with commercial terms, if any within due dates for Managed Services provided herein by SDC.

5.3. To provide promptly all information and documentation for obtaining their clearance/approval and authority to co-ordinate with vendors for warranty etc. wherever required

5.4. Subscriber shall not, directly or indirectly open, alter, try to hamper with or in any way do any act which will result in interfering with the internal operation of the system and do any modification to the configuration supplied by SDC without prior written approval of SDC and without the presence of SDC representative.

5.5. Subscriber shall nominate a nodal officer for coordination with SDC. All communication to SDC should be through the nodal officer and vice-versa.

Signature Signature

KSITM Director

5.6. Provide technical and operational manuals for all equipment to be installed and arrange for the shipping of hardware, cabling (labeled), cabling ties, and all other material needed to install the equipment

5.7. Configure the hardware and install all software and SLA management of all installed equipment and software.

5.8. Subscriber shall get system audit and security audit of the application done through CERT-IN empaneled agency and produce “safe for hosting” certificate before go live of the application. Subscriber shall also undertake to get security audit of the application done at regular intervals or as and when changes are made to the application. SDC recommends security audit of the website once in a year or whenever major changes are made to the applications.

5.9. Data backup and system and application security shall be the responsibility of the Subscriber. Subscriber shall apply all relevant software updates and patches as and when required

6. **Complaint Management:** The Subscriber shall follow the following procedure for lodging the complaint in relation to the Managed Services:

6.1. The complaint management activity will be carried out through SDC Help Desk.

6.2. The Subscriber should call and email the Managed Services Help Desk for SDC-1 at 0471 2317618, 2728618 sdc1.ksitm@kerala.gov.in and SDC-2 at 0471-2700272 or 0471-2700270. sdc2.ksitm@kerala.gov.in to record the complaint. Any change in the number or e-Mail will be notified immediately to Subscriber

6.3. The Technical contact person of the Subscriber while lodging the complaint shall indicate the nature of fault.

6.4. The ticket No. should be referred for any enquiry for ascertaining the status of complaint till the problem pertaining to the Complaint has been solved.

Typically, SDC intends to respond to the most critical problems, those that disable current business operations— and assign them to a specialist.

Emergency requests are defined as issues that affect the inability to conduct business.

Signature Signature

KSITM Director

7. DISCLAIMER & LIMITATION OF LIABILITY

SDC does not make any formal or implied claim of the Product or services to control all attacks, misuse of network or loss of data in Subscriber's Network System after the Product is installed, and further Subscriber accepts that

IN NO EVENT SHALL KERALA STATE DATA CENTRE (SDC) OR KSITM BE LIABLE FOR INCIDENTAL CONSEQUENTIAL, SPECIAL OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF THE USE, MISUSE, OR ANY APPLICATION OF THE SAID PRODUCT EVEN IF KERALA STATE DATA CENTRE (SDC) IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL KERALA STATE DATA CENTRE (SDC) OR KSITM BE LIABLE FOR ANY CLAIM, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY WHETHER MADE BY OR ON BEHALF OF THE USER, OR ANY THIRD PARTY.

8. **TERMINATION**:

8.1. Service must be subscribed for a minimum period of three years. In case the subscriber terminates any service prior to the completion of one year, charges as agreed to (clause 6 above) for one year shall be borne by the Subscriber. However if Subscriber wishes to terminate services after the completion of one year, it can do so by giving one-month prior notice.

8.2. If at any time during the term of this Agreement, either Party fails to perform its respective obligation ("Defaulting Party") under this Agreement, the other Party ("Non-defaulting Party") shall have the right to terminate this Agreement by giving to the Defaulting Party a written notice setting out the breach of obligation complained of ('Breach'). The notice of termination shall have effect and this Agreement shall stand terminated upon expiry of 90 (ninety) days of such notice of termination if the Defaulting Party fails to cure the Breach within 60 (sixty) days of receipt of the notice of termination.

8.3. Upon termination of this Agreement, SDC shall hand over within 30 days, all and any reports prepared up to the date of termination as also all documents and files containing Confidential Information pertaining to the Subscriber in connection with the Managed Services in its possession except the Confidential Information that is required to be maintained by SDC pursuant to the law, regulation or direction as the case may be.

9. **ARBITRATION AND JURISDICTION**:

9.1 In the case of any dispute or claim arising out of or in connection with or relating to this Agreement, or the breach, termination or invalidity hereof, the parties shall try to resolve the dispute amicably.

9.2 Should such dispute or claim etc. remains unresolved for a period of thirty (30) days the same shall be referred to the Secretary, Information Technology, Government of Kerala whose decision shall be binding on both parties

----

Signature Signature

KSITM Director

9.3 This Agreement shall be governed by and construed in accordance with the laws of India and courts at Trivandrum shall have exclusive jurisdiction.

10. **CONFIDENTIAL & PROPRIETARY INFORMATION**:

The Parties will keep the Confidential Information as also the terms of this Agreement strictly confidential during the term of this agreement. Should any disclosure be required to be made by law (including, but not limited to, court order, legal process, or governmental action) or otherwise, then the Party receiving such notice shall promptly inform the other Party of such notice or request so that the Party to whom the notice has been given may seek, at its expense, an appropriate protective order or waiver of compliance of this Clause. If, in the absence of a protective order or waiver, the Party in the opinion of its counsel, is compelled to make disclosure such Party may make such disclosure after notice to the other Party.

The provisions of Clause shall not applicable if: any Confidential Information

(a) Is already known to a Receiving Party, or

(b) Which becomes available to a receiving Party from other sources which the disclosing Party reasonably believes not to be bound by any obligation of confidentiality, directly or indirectly, to the receiving Party, or

(c) Which is independently developed by a receiving Party or

(d) Which is now or hereafter available to the public without breach of this Agreement by either Party, or

(e) This is disclosed outside with the prior written approval of the receiving Party.

Signed & delivered on behalf of SDC. Name : Place	Signature & Stamp
Signed & delivered on behalf of the subscriber. Name : Place	Signature & Stamp

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the date first above written.