Hosting protocol

for

Co-Hosting, Co-Location & Cloud Services at Kerala State Datacenter

Kerala State IT Mission

Department of Electronics & Information Technology, Government of Kerala

Introduction

State Data Centre (SDC) has been identified as one of the important element of the core infrastructure for supporting e-Governance initiatives of National e-Government Plan (NeGP). State Data Centre would provide many functionalities and some of the key functionalities are central data repository of the State, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Portal, Service Integration etc. These services shall be rendered by the States through a common delivery platform supported by other core infrastructure elements i.e. State Wide Area Network (SWAN) and Common Service Centres (CSC). The State Data Centre is a key supporting element of e-Government initiatives for delivering services to the citizens with greater reliability, availability and serviceability. The State Govt. departments would get a seamless, highly reliable, robust, shared and a secured data centre infrastructure with reasonable capacity for deploying their e-Governance applications. The State Data Centres are identified as one of the Critical Information Infrastructure (CII).

This document is intended to cover various protocols and procedures to be followed by the Govt. Departments for the safe and secure hosting of the websites, applications at the Kerala State Data Centre as soon as when they are ready to deploy.

Present Infrastructure of Kerala State Data Centre (KSDC)

Government of Kerala have two State Data Centres which were functioning at 4th floor, Co-Bank Towers, Palayam and Thejaswini Buildings, Technopark in Thiruvananthapuram district which were established in the year 2005 and 2011. The Kerala State Data Centre (KSDC) would provide a secure and physical infrastructure including rack space, power with UPS & generator backup, air conditioning, fire prevention, access control mechanism etc. with a guaranteed minimum uptime of 99.5%.

The networking facilities, firewall, Antivirus, storage, load balancers, VPN etc. would be provided for the servers or applications for securely and efficiently delivering the services to web or intranet. Shared infrastructure includes database, application and web servers would enable the Govt. departments to host their e-governance applications. Cloud infrastructure is already in place at both the State Data Centres which would provide dedicated virtual machines to host the applications and the hardware resources can be augmented based on the demand.

SERVICES OFFERED

These are the various services available from KSDC which can be availed by the Government Departments. The services are broadly classified as

1. Co-Hosting Services
2. Co-Location Services
3. Cloud Hosting Services
4. Helpdesk Services

1. CO-HOSTING SERVICES

Departments can host their applications in the servers that are being managed by KSDC. A shared infrastructure will be provided to the departments and the responsibility of managing the servers, database and storage will be with Data Centre Operator (DCO).

1. To avail the co-hosting services, the department shall submit a signed copy of the Co-hosting application form to the Director, Kerala State IT Mission (KSITM). The application form can be downloaded from the official website of https://itmission.kerala.gov.in/downloads.
2. Department need to fill in all mandatory fields mentioned in the Co-Hosting form. Partially filled forms will not be accepted. Department need to submit the software architecture and the programming language version details along with the form.
3. KSITM will verify the application form and if accepted, necessary instruction will be given to the Data Centre Operator (DCO) for hosting the application in KSDC and this will be communicated to the Department.
4. DCO will create a service ticket for the case, and the status of the ticket will be informed to the Department. Any clarifications regarding the architecture, version of software, contact information etc. will be clarified by the DCO during the provisioning.
5. The list of available software / framework / platforms for hosting will be available from the official website https://itmission.kerala.gov.in/downloads.
6. DCO will review the update the software / platform every six months or whenever there is a major update available and provide a test platform for the departments to migrate and test the application to the latest platform.
7. It is the responsibility of the Department to migrate the application to the latest stable platforms to avoid security breaches due to unsupported versions / vulnerability etc. in the older platforms. In the case of unsupported/ vulnerable versions of software, if found KSDC will notify the department and proceed with the quarantine of the application and the public access of the website / application will be revoked till the department has taken necessary remedial measures for fixing the vulnerabilities.

8. KSDC will provide a staging environment to the departments for testing the application and doing the security auditing. In the staging environment, only limited intranet/internet static IP of the Department / Security Audit Agency / Development team will be permitted, and the website / application will not provide public access.
9. When the application is in the staging environment, department need to perform a security audit from a CERT-In empanelled agency, and the costs for the audit has to bear by the concerned department. (Note **: Department can avail the staging space for a maximum period of 6 months. If they are not moving to production even after 6 months, then KSDC will decommission the space / block the access to the staging without prior notice).
10. Once the security audit certificate is obtained from the CERT-IN empanelled agency, Department has to forward the copy of the certificate to KSDC for moving the application to the production servers. KSDC will verify the audit certificate and grant the permission to go live with the approval of KSITM / CT team.
11. Whenever department plans for revamping the application following steps need to be adhered to.

    Major Updates:

    - The Department need to make changes in the provided staging space and test it properly.
    - The Department need to fill in the change request form and submit the same to KSDC along with the updated application architecture.
    - The application needs to undergo the security audit within the staging environment, department need to procure an audit certificate from CERT-IN empanelled agencies. Audit performed in another environment is not accepted.
    - KSDC will perform the production switching by initiate a change ticket and schedule down time as per approval from the department.

    Minor Updates:

    - The Department need to make changes in the provided staging space and test it properly.
    - The Department need to fill in the change request form and submit the same to SDC along with the details of update.
    - Upon receiving the change request from department KSDC will schedule down time for switching to the new version.
12. Departments are responsible for the revamp of the website / application to support the latest stable versions of the Operating System/Content Management System(CMS) platforms.
13. The Department need to re audit their application whenever the application undergoes major changes and submit the updated certificate to KSDC.

14. KSDC team will take weekly backup of application as well as databases (retention period 30 days).
15. It is the responsibility of the department to intimate KSDC whenever there is a change in the contact details of the organization.
16. SSL certificate is mandatory for all the web applications available from internet. KSITM has already procured wild card certificate for *.kerala.gov.in domain. Department needs to contact with KSDC for installing the same for their websites.
17. If the department requires domain name registered under kerala.gov.in. , they need to submit the application for domain registration which is available from https://itmission.kerala.gov.in. The application for domain registration shall be submitted to the Director, Kerala State IT Mission.

2. CO-LOCATION SERVICES

KSITM will provide a co-location space at the KSDC to the Departments for hosting their servers, storage and related infrastructure. The required space, power, air-conditioning, security etc. will be provided by KSDC and the responsibility of managing the servers, storage and the related infrastructure co-located shall be with the concerned Department. Co-location is permitted to the departments, if prior approval from KSITM is obtained before the purchase of the items, and only based on availability of sufficient infrastructure.

1. Department shall prior consult with Kerala State IT Mission regarding the space availability, Power supply requirements, Storage requirements, Network feasibility etc. before the procurement of the servers, storage and related hardware's which are planned to be installed at KSDC. Approval from KSITM has to be obtained, by the concerned department before proceed with the purchase of items.
2. KSITM will permit the co-location of the servers and storage, if the requirement of the department doesn't fit with the present cloud infrastructure available at KSDC.
3. If the Department didn't take prior approval from KSITM, the co-location application will be summarily rejected and will be communicated to the Department.
4. To avail the co-location services, the department shall submit a signed copy of the Co-location application form to the Director, Kerala State IT Mission (KSITM). The application form will be available from the official website https://itmission.kerala.gov.in/downloads.
5. Department need to fill in all mandatory fields mentioned in the Co-location form. Partially filled forms will not be accepted. Department need to submit the application details, architecture and the programming language version details along with the form.
6. KSITM will verify and approve the request and forward the same to KSDC for further provisioning of infrastructure.
7. KSDC will assign service ticket in the service desk tool and intimate the department. Any clarifications regarding the architecture, version of software, contacts etc will be clarified and corrected before allocation of the service.

8. Department will be responsible for server/device mounting, installing software's, clearing package boxes, replacement of disks etc without causing any disturbances to the existing infrastructure.
9. The representatives from the Department need to be available at the KSDC during the mounting of devices, installations, verifying the assets and completing other data centre formalities.
10. In order to monitor the system health and resource usage, KSDC will add the devices to the NMS DARPAN Monitoring tool. (Note**: Any outage in the server connection will be intimated to the department based on the alerts from DARPAN). KSDC will provide the steps for SNMP configuration and department needs to configure the same on each device. The NMS discovery is mandated to all the existing as well as new servers and the public access to the application will be permitted only after completion of this activity.
11. Department need to produce the safe to host certificate for the application from a CERT-IN empanelled agency for opening the website to public domain.
12. The Department need to inform KSDC before doing any changes in live application. (Such as Operating System, CMS versions upgrade etc.).

Major Changes:

The Department need to fill in the change request form and submit the same to KSDC along with the updated application architecture. Department need to make changes in the server (other than production) with in KSDC and security audit using CERT-IN empanelled agency to be performed for getting the safe to host certificate.

- KSDC will check and review the change request along with updated application architecture and seek any clarifications from department if required. (Department need to submit the updated architecture and all new updated version details along with the form)
- KSDC will initiate a change ticket and schedule a down time for switching the older site to new. (Note: department need to inform the down time in their official site)

Minor changes:

The Department need to fill in the change request form and submit the same to KSDC along with the updated application architecture. Department need to make changes in the server (other than production) and inform to KSDC.

- KSDC will check and review the change request along with updated application architecture and seek any clarifications from department if required. (Department need to submit the updated architecture and all new updated version details along with the form)
- KSDC will initiate a change ticket and schedule a down time for switching the older site to new. (Note: department need to inform the down time in their official site)

13. Departments need to perform a re-auditing of the live application using a CERT-IN empanelled agency at least once in every two years. KSDC will sent a email intimation and three months time will be given to produce the re audit certificate, if the department still fails to present the certificate in the time interval then the public access to the application will be revoked by KSDC, upon confirmation from KSITM.
14. Department need to update / patch the Operating Systems and software periodically. If the Operating Systems, CMS, or software's found vulnerable KSDC will send email intimation with 30 days of lead time to update the system, if the department still fails to present the certificate in the time interval then the public access to the application will be revoked by KSDC, upon confirmation from KSITM.
15. The tape backup services, load balancing, VPN, managed security services will be provided only based on the request from the department.
16. It is the responsibility of the department to intimate KSDC whenever there is a change in the contact details of their organization.
17. KSITM reserves its right for the removal of unused, idle, obsolete resources from KSDC, under intimation to the Department. The Department shall take necessary actions for the removal of obsolete devices from KSDC within 30 days of request or else KSITM will terminate the services and de-allocate the said resources to free up the space and no claim will be entertained in future. The cost for the removal will be recovered from the respective department.
18. KSITM will have the right to share the resources (Servers, Storage) to other departments in case if the servers / storage are found to be underutilized or on need basis under intimation to the concerned department.
19. The server racks purchased by the Departments which are placed at KSDC will be part of the common infrastructure and KSITM reserves its right to allocate space to the Departments based on availability, without any prior permission from the Department.
20. The co-located space is provided for a period of one year which is to be renewed annually by the Department if they are being used, or else will be decommissioned by KSDC upon intimating the Department. The Department has to remove the co-located devices from KSDC upon request from KSITM at their own cost.
21. Departments shall plan migration of the applications currently hosted in the co-located environment to the cloud infrastructure to the possible extent.
22. KSITM will not permit the Department to keep their obsolete servers or other hardware at KSDC, after the service life due to safety and security reasons.

3. CLOUD HOSTING SERVICES

Departments can host their websites or applications in the virtual cloud servers that are being managed by KSDC. A shared cloud infrastructure will be provided to the departments and the responsibility of managing the cloud servers, database and storage will be with Data Centre Operator (DCO).

1. To avail the cloud hosting services, the department shall submit a signed copy of the Virtual infrastructure application form to the Director, Kerala State IT Mission (KSITM). The application form will be available from the official website https://itmission.kerala.gov.in/downloads.
2. Department need to fill in all mandatory fields mentioned in the application form. Partially filled forms will not be accepted. Department need to submit the software architecture and the programming language version details along with the form mandatorily.
3. KSITM will provide the staging space for the virtual cloud infrastructure for the new VM applications as per the following configuration. The staging environment will be provided for a period of 3 months initially which is extendable to a maximum of 6 months. The staging environment is provided only for performing the security audit and the testing of the application from a limited number of IP address. In the staging environment, KSITM will not provide more than 2 VMs to a single application unless there felt a substantial requirement, based on the application architecture.

Category	**vCPU**	**RAM**	**Storage**
Web/ Application server	4	8	100 GB
Database Server	4	8	100 GB

1. If the storage, memory and CPU requirement is above the normal provision rate, then the Department shall justify the requirement with all relevant details or else will be rejected.
2. KSITM will verify the application form and if accepted, necessary instruction will be given to the Data Centre Operator (DCO) for providing the cloud infrastructure in KSDC and this will be communicated to the Department.
3. DCO will create a service ticket for the case, and the status of the ticket will be informed to the Department. Any clarifications regarding the architecture, version of software, contact information etc. will be clarified by the DCO during the provisioning.
4. KSDC will notify the department prior 15 days before the date of expiry. The staging space will be decommissioned by KSDC after the expiry period of 3 months, and it is the responsibility of the department to take back up of the data and application which is residing on the mentioned servers. If the department want to continue the hosting, they need to submit the cloud renewal application form, for a period of further 3 months. KSITM will not provide further extension beyond a period of 6 months, unless there felt necessity.
5. Once the Department completed the security audit and produced the safe to host certificate from a CERT-IN empanelled agency for the deployed application in staging, then the application will be moved to production environment and public access will be given.

6. In order to monitor the system health and resource usage, KSDC will add the devices to the NMS DARPAN Monitoring tool. (Note**: Any outage in the server connection will be intimated to the department based on the alerts from DARPAN). KSDC will provide the steps for SNMP configuration and department needs to configure the same on each device. The NMS discovery is mandated to all the existing as well as new cloud virtual servers and the public access to the application will be permitted only after completion of this activity.
7. Additional server resources (vCPU, Memory and Storage) will be provided only if the allocated resource utilization reaches 70% or above based on the NMS reports or in case of any genuine reasons subject to approval from KSITM. The cloud revision request form shall be submitted by the Department for increasing the server resources.
8. The cloud resources which are in production environment are provided for a period of one year which are to be renewed annually by the Department if they are being used, or else will be decommissioned by KSDC upon intimating the Department. The Department has to take the backup of the application and database if required, and KSDC will not be held responsible for the same.

4. HELPDESK SERVICES

Kerala State Data Centre (KSDC) is providing a 24x7x365 helpdesk services to the Departments, for addressing the complaints, service requests, incident handling, support services etc.

	Contact Number	**Email**
Helpdesk Services	0471-2728618,2317618	sdc.ksitm@kerala.gov.in

Service Window

Severity Level	**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

- - 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.

1. KSDC will create a service ticket for each requests coming to the email address, or through phone and inform the details to the concerned requester.
2. In the case of any escalation of complaints related to KSDC, Departments may communicate to the Asst. Mission Co-ordinator, Kerala State IT Mission (Email: subil.ksitm@kerala.gov.in)

GENERAL TERMS AND CONDITIONS

1. Security auditing is mandated for all the websites / applications which are hosted in co-located, co-hosted and cloud virtual infrastructure at KSDC. It is the responsibility of the concerned Department to perform the security auditing by a CERT-IN empanelled agency, at the time of deployment of application to public and periodical audit to be conducted once in every two years. The costs for the security audit have to be borne by the concerned Department.
2. The Department will be held responsible for the fixing of any vulnerability if noticed in the application or servers in the case of co-located and cloud virtual infrastructure.
3. The Department shall take best efforts to secure the web servers, application and the database servers from the vulnerabilities and doing a periodic check every 3 months on server hardening in the case of co-located and cloud virtual infrastructure.
4. The Department shall inform KSDC about the details of the websites and applications hosted in the co-located and cloud virtual servers whenever there a new application/website is hosted in the servers being managed by them.
5. If KSITM noticed any old / unsupported vulnerable version is being used in the servers managed by the Department, KSITM will intimate the Department to fix the issues with a stipulated time or else the public access will be blocked till the issue is fixed.
6. As part of KSDC security audit process, the Third Party Auditor (TPA) will carry a periodic security audit on the servers and identified applications which are hosted at the KSDC. All the Departments shall provide the details of the application, any other information as required for the TPA to complete the security auditing the application, necessary access permissions upon request from KSITM.
7. The list of vulnerabilities, if any found during an audit performed by KSITM/TPA/CERT-K will be communicated to the Department, and the Department shall take necessary corrective actions to fix those vulnerabilities within 30 days time or else KSITM will terminate the services to the website/ application till the vulnerability is fixed.
8. KSITM will immediately block the public access to the servers, if noticed a serious security breach or threat and KSDC will communicate this to the concerned Department.
9. Any incidents related to hacking, malware infections etc. for the websites hosted under KSDC shall be reported to sdc.ksitm@kerala.gov.in., cert.ksitm@kerala.gov.in, immediately by the department.
10. KSDC will provide the server antivirus licenses to the Departments based on request. Departments can contact the KSDC helpdesk for getting the necessary licenses and support.

11. KSDC will provide the Web Application Firewall services to the Departments on request, which will provide additional security to the web applications hosted.
12. KSDC will provide the VPN services to the Departments on request, for accessing the web applications / servers remotely.
13. KSDC will provide the Tape backup services to the Departments on request, for which Departments can contact the KSDC helpdesk.
14. If the department requires domain name registered under kerala.gov.in. , they shall submit the application for domain registration which is available from https://itmission.kerala.gov.in. The application for domain registration shall be submitted to the Director, Kerala State IT Mission.
15. SSL certificate is mandatory for all the web applications available from internet. Department shall purchase and install SSL certificate in the application servers, in a co-located environment and cloud virtual infrastructure since these are being managed by the Department.
16. Department shall submit the request for co-hosting / co-location / cloud hosting if the applications are ready for testing and deployment. Idling of the provisioned resources will lead to termination of services and further requests from the Department will be considered only after decommissioning the idle resources.
17. It is the responsibility of the respective Department to timely inform KSITM / DCO on the decommissioning of the resources (Co-hosted / Co-located / Cloud Hosting) if they are unused to optimise the resource utilization of KSDC.

....