1 Hosting of Websites/Web application Procedure

1.1 About the Service

As per the policy decision, all the departments are required to host their Websites/Portals/Applications at State Data Center only. The State Data Center is equipped with state of the art facilities for hosting websites/web-based applications/portals. Following options are available to host at State Data Center -

i. **On a shared basis:** The departments may deploy their websites using existing infrastructure available at SDC in terms of servers, system software etc. The list of IT infrastructure presently available at SDC for this purpose is annexed at **Annexure 2.1.** To avoid any delay on account of procurement of additional hardware/software, the departments are advised to develop their websites/applications/portal in such a manner that the existing infrastructure available at SDC can be utilized for hosting purpose.

ii. **Dedicated Infrastructure**: The Departments may be allowed to install their dedicated servers and software at SDC for hosting their web sites. In such case, departments would be required to procure and install the required hardware/software at State Data Center. Facility Management Service will be provided by the SDC operator. It should be noted that the procured servers should be Rack mountable only. DoIT&C should be consulted before finalising the technical specifications.

1.2 Service deployment Architecture

The picture below depicts a typical 2-tier architecture i.e. having militarized zone & de-militarized zone. Firewalls are placed between every two tiers to enable network perimeter security.

(i) Internet Zone

In this zone, the Internet leased line is terminated. The users come through the internet cloud in this zone to access the web sites hosted at SDC.

(ii) Demilitarized Zone

In this zone, all the web servers, applications servers and DNS servers are installed at State Data Center. A firewall is installed between the Internet Zone and demilitarized zone to protect the web/application servers from any security threats through Internet Zone.

(iii) Militarized Zone

The Militarized Zone of State Data Center consists of two segments i.e. Database Server Zone and LAN/WAN User zone. Both the Segments are isolated from each other through a Firewall to protect the Database Servers from any security threats from LAN/WAN users. To protect the Militarized zone from any external threats from

the Internet Zone, the Militarized Zone is also separated from Demilitarized zone through a Firewall. No access is provided to the militarized zone except from Network operation center (NoC).

The Pictorial representation of the Deployment Architecture of State Data Center is as under:

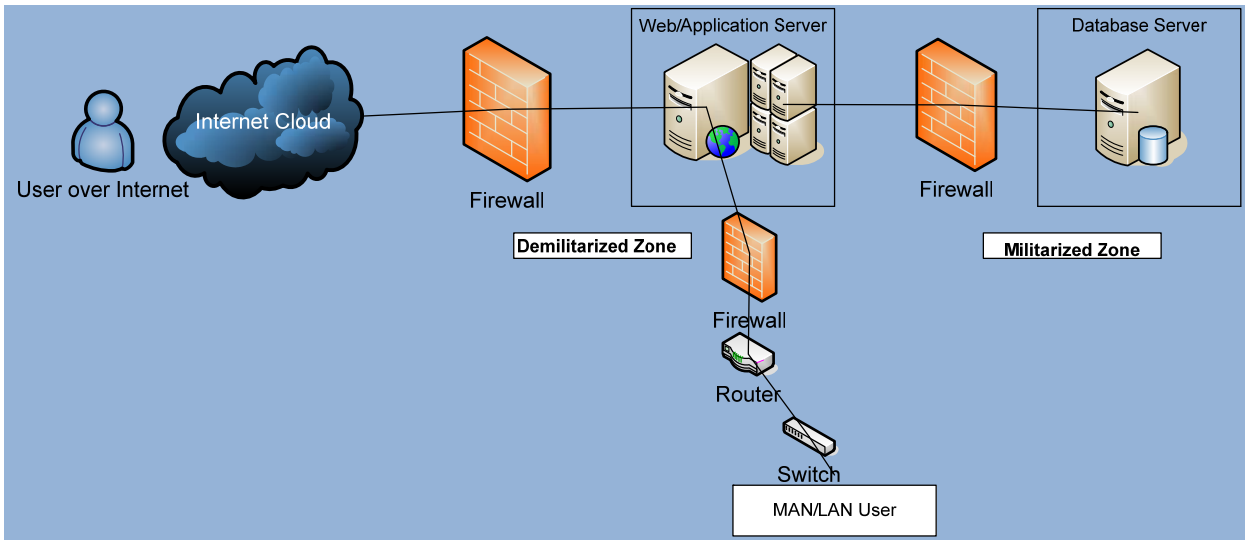

Fig: *Deployment Architecture of State Data Center*

1.3 How to avail the service?

Following procedure has to be followed by all the Departments to avail this service-

Step-1: The Departments are required to get their Web Site/Portal/Application certified as "SAFE TO HOST" from any certifying agency as approved by Government of India like STQC. The latest list of certifying agencies approved by Government of India can be obtained from official web site of CERT-IN(Indian Computer Emergency Response Team) i.e. http://www.cert-in.org.in/panelofauditors.htm.

DoIT&C can also provide funds for the same.

Step-2: After obtaining the SAFE to HOST Certificate for proposed web site/application/portal, the departments shall submit their request for hosting it at State Data Center to Commissioner, Department of IT&C, Yojna Bhawan, Tilak Marg, Jaipur in the prescribed format along with the CD containing soft copy of the website/application/portal and deployment manual. The format of Request form is available at **Annexure-2.2**.

Step-3: On receipt of the request from a department, the Department of IT &C would evaluate the request on the basis of the procedure as defined in **Annexure 2.3**. In case the proposal is found feasible for hosting at SDC, DoIT&C shall host the website. ***Post the approval of feasibility report by DoIT&C,*** *Departments are required to depute*

their technical representative at SDC to facilitate/assist DoIT&C in hosting the website/application/portal.

1.4 What is provided at the State Data Centre ?

i. In Scope

- Sub-Domain Creation under rajasthan.gov.in
- DNS entries of domains in DNS servers installed at SDC
- Content Deployment on the web/Application/Database server
- Information Security as per SDC Policy
- Precision power to all racks
- Precision Air Conditioning (PAC)
- Server space
- Facilitating transit of equipment into and from Server Farm; receipt of the hardware (only main item not full & detailed specifications) once it is installed in Server Farm will be provided.
- LAN connectivity, if required.
- FTP-User-ID with password for web-sites for content management remotely / outside the SDC; permission to enter SDC will be given selectively only .
- Email addresses with password subject to availability on email server (user and user-id)
- Assistance to get the ITES / ITC equipment installed up to certain extent as per agreement executed between the DoIT&C and FMS vendor
- The Server Farm resources such as power, PAC, connectivity etc. shall be mobilized depending upon their availability.
- Provide services related FMS and O&M. The department would have to pay 6% of the total CAPEX for the services.

ii. Out of Scope

a. General

- Domain Registration
- Application Development
- Content Creation/edit
- Application level security (coding)
- Application level tuning /troubleshooting
- Shifting of servers from one Zone to another Zone
- Remote administration on database server

b. In case IT Infrastructure is provided by Department

- Rack mountable hardware
- General Maintenance of IT Infrastructure
- Facility Management of IT Infrastructure, if any
- Insurance of IT Infrastructure
- Annual Maintenance of IT Infrastructure

F. Annexure(s) to be referred by the Department and FMS, SDC

The documents/Annexure(s) used/filled for the service delivery are mentioned in the table below.

S.No	Annexure Name	Action by	Annexure Number
1.	List of IT Infrastructure at SDC	-	2.1
2.	Website/Portal/Application Hosting Requisition Form	Departments	2.2
3.	Evaluation Procedure for Hosting	DoIT & C	2.3
4.	Hosting Details Record	FMS,SDC	2.4
5.	Fulfillment of Request	DoIT&C	2.5
6.	Request for Routine work and Extra Privileges	Departments	2.6
7.	Feasibility Report	FMS,SDC	2.7
8.	Website Hosting Checklist *(for FMS,SDC only)*	-	2.8

1.5 Role of the Beneficiary Department

i. Bringing ITES / ICT equipment / infrastructure into SDC through staging room and subsequently to the server farm.

ii. It is the responsibility of the Department concerned which is bringing in its h/w, s/w and other accessories in SDC, to fit in appropriate rack (assigned or owned) as per industry standards and according to their need.

iii. Arrangement of sufficient number(s) of 42 U rack which can be shared by DoIT&C, if not available in the State Data Center

iv. Installation, commissioning and integration of ICT equipment whenever it is required to be redone, if ever.

v. Provide insurance of ITES / ICT equipment-n-infrastructure brought into the SDC and maintain their continuity (documents are attached as per Annexure No. 2)

vi. Person(s) responsible for the project should bear valid photo-ID-Proof and show the same as and when asked while entering into SDC area

vii. Provide details in writing what has been done in server farm. However, the Department is responsible for their ITES / ITC infrastructure and its working (details in Annexure-6)

viii. Department shall maintain warranty and AMC of the equipment / services installed in SDC (documents are attached as per Annexure No. 2.2)

ix. Termination of all kinds of connectivity required at the desired place

x. To make arrangements for Internet bandwidth of sufficient denomination and their recurring expenses, if demanded

xi. Provide and install all kinds of required licenses and maintain their continuity

xii. Provide the name of Nodal Officer / Coordinating Officer with complete contact details who can be contacted at any time, (as per Annexure No. 2.2)

xiii. Department shall be responsible for updation of website free from application level vulnerability and with time-stamp. DoIT&C shall not in any case, be responsible for the content of the website/web-application.

xiv. Setting up of “Site Under Maintenance” page during routine maintenance of the site/ portal/ application so that users can know that the website is being updated / maintained at that time.

xv. The Website/Web-Application must carry “Safe-To-Host” certificate and its continuity (attach document at Annexure No. 2.2)

xvi. Department has to abide by all the laws of land.

1.6 User Web Site/Application Content

The Departments are solely and fully responsible for all information, data, text, software, music, sound, photographs, graphics, video, messages, goods, products, services or other materials ("Content"), whether publicly posted or privately transmitted using the Service or a User Web Site. DoIT&C does not pre-screen content, but it and its designers shall have the right (but not the obligation) in their sole discretion to refuse or remove any content that is made available to others using the Service or on a User Web Site. DoIT&C neither endorses the content of Department’s User Web Site nor assumes responsibility for such content. Departments must evaluate, and bear all risks associated with, the use of any content, including any reliance on the accuracy, completeness, or usefulness of such content.

The following is a non-exclusive list of activities prohibited under this policy:

i. The uploading, posting or otherwise transmitting of any content on a User Web Site that is unlawful, harmful, threatening, abusive, harassing, torturous, defamatory, vulgar, obscene, libelous, hateful, racially, ethnically or otherwise objectionable, or violates privacy, publicity or other personal rights of others;

ii. Sending unsolicited bulk and/or commercial messages over the Internet to a large number of recipients (known as "spamming"), or maintaining an open SMTP relay. This prohibition extends to the sending of unsolicited mass mailings from another service that in any way implicates the use of the service, DoIT&C's equipment or any domain name registration or electronic mail address serviced by DoIT&C;

iii. The forgery of any headers or other manipulation of identifiers in order to disguise the origin of any message sent in connection to a User Web Site;

iv. Using the Service to harm minors in any way, including advertising, transmitting, store, post, display, or otherwise making available child pornography.

v. The uploading, posting or other transmittal of any content that violates, infringes or misappropriates the intellectual property rights of others, including patents, trademarks, service marks, trade secrets, copyrights or other proprietary rights of any party;

vi. The uploading, posting or other transmittal of any content that you do not have a right to transmit under any law or under contractual, fiduciary or personal relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements);

vii. Using the Service to create, upload, post or transmit any viruses, worms, Trojan horses, or for pinging, flooding, mail bombing or denial of service attacks or any other malicious computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment;

viii. Attacking or attempting to gain unauthorized access to the data, computers, accounts, systems or networks of others, or attempting to penetrate security measures of DoIT&C or other entities' systems ("hacking"), or engaging in any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, probe, or other information gathering activity);

ix. Installation of 'auto-responders', 'cancel-bots' or similar automated or manual routines that generate excessive amounts of net traffic, or disrupt net newsgroups or email use by others.

x. Engaging in activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service, or equipment;

xi. Violating any local, state, national or international laws;

xii. Engaging in or promoting gambling;

xiii. Displaying or promoting any type(s) of intoxicant, alcoholic beverage, cigarettes or drug, where prohibited by local, state, national or international law;

xiv. "Stalking" or otherwise harassing another;

xv. Collecting or storing personal data about others without their consent;

xvi. Advocating, promoting, or providing assistance in carrying out violence or physical harm against any persons, nations, groups, entities or animals, including providing instructions on how to assemble explosive devices or other weapons, describing or displaying a weapon, parts of weapons or manuals for assembling any weapon, or promoting products or services that involve a significant risk of death or injury to any persons, or damage to business or other entities or property;

xvii. The use of your User Web Sites as storage for remote loading or as a door or signpost to another home page;

xviii. The impersonation of any person or entity, including, but not limited to, a DoIT&C official, forum leader, guide or host, or falsely stating or otherwise misrepresenting your affiliation with a person or entity;

xix. Removing, modifying or hiding any of the advertising banners inserted into your User Web Sites;

xx. Any resale or any exploitation for any commercial purposes of the Service by any and all means unless approved in advance in writing by DoIT&C; and

xxi. Advertising, transmitting, offering for sale or otherwise making available any software, program, product, service or information that is designed to violate terms (a) through (u) above, or that DoIT&C determines, in its sole discretion, is inappropriate for sale through the Service provided by DoIT&C.