Website Hosting Requisition form

For Hosting Website / Portal / Applications at State Data Centre

Department of Information Technology and Communication

Government of Rajasthan

Form No. (*To be filled by DoIT&C*)			**Date of submission**	
1.	**Organization Details**			
1.1	Name of Department/Organization			
1.2	Name of Nodal Officer			
1.3	Designation			
1.4	Phone No. (Office)			
1.5	Phone No. (Mobile)			
1.6	e-Mail Address			
1.7	Postal Address			
2	**Application Details**			
2.1	Sub Domain proposed by Department			
2.2	Required Domain Name other than rajasthan.gov.in			
2.3	Application Type (Pl. Tick your response)	External Open to public (……..) Or Internal Network (Only for SecLAN) (…….)		
2.4	Type of the application	Website [ ]	Portal [ ]	Application [ ]
2.5	Nature of the application	G2G [ ]	G2B [ ]	G2C [ ]
2.6	Administrative approval obtained for Hosting the site at SDC	Yes [ ]	No [ ]	
2.7	User Acceptance Test (UAT) approved by Department	Yes [ ]	No [ ]	
2.8	Hardware Type (Pl. Tick your response)	Dedicated (provided by dept) (……..) Or Shared (……..)		

3	**Application Developed by**			
3.1	Name of the Company / Agency			
3.2	Name of Contact Person			
3.3	Address of Contact Person			
		Pincode :		
3.4	Phone No. (Office)			
3.5	Phone No. (Mobile)			
3.6	e-Mail Address			
4	**Application being Maintained by**			
4.1	Whether Website/Application is Under Maintenance	Yes [ ]	No [ ]	Expiry:
4.2	Name of the Company / Agency maintaining the Web Site/Application			
4.3	Name of Contact Person			
4.4	Address of Contact Person			
4.5	Phone No. (Office)			
4.6	Phone No. (Mobile)			
4.7	e-Mail Address			
4.8	Contract Copy(ies) attached	Yes[ ]	No[ ]	
5	**Facility Management being provided by** *(In case of Dedicated Hardware)*			
		FMS (Facility Management Services)		**AMC (Annual Maintenance Contract)**
5.1	Hardware Under FMS/AMC	Yes[ ]	No[ ]	Yes[ ] No[ ]
5.2	Name of the Company / Agency			
5.3	Name of Contact Person			
5.4	Address of Contact Person			
5.5	Phone No. (Office)			
5.6	Phone No. (Mobile)			
5.7	e-Mail Address			
5.8	Contract Expiry Date			
5.9	Contract Copies attached	Yes[ ]	No[ ]	Yes[ ] No[ ]

6	**Hardware Specifications (In case of dedicated h/w provided)**		
6.1	Name Make/ Brand		
6.2	Model Type		
6.3	Hardware Description	**CPU :** **RAM:** **HDD:** **HBA card:** Yes[ ] No[ ] **Fiber Cable:**	
6.4	Power Consumption Details (Amp /watt)		
6.5	Rack Provided	Yes[ ] No[ ] Type (if Yes): Server / Network	
6.6	Copy of Insurance	Yes[ ] No[ ]	
6.7	Antivirus Type with Expiry	Name: Expiry Date:	
6.8	PO attached	Yes[ ] No[ ]	
6.8	Any Special Hosting Environment required		
7	**Application Hosting Environment required by Department**		
7.1	**Minimum Hardware requirements** *(In case of shared Infrastructure)*		
7.1.1	Web Server Configuration	1. Processor : 2. RAM : 3. Storage Space :	
7.1.2	Application Server Configuration	1. Processor : 2. RAM : 3. Storage Space :	
7.1.3	Data Base Server Configuration	1. Processor : 2. RAM : 3. Storage Space :	
7.1.4	Any Other Server Required-Also Specify the Usage		
7.2	**Software requirements for hosting**		
7.2.1	Operating System of Web Server with Version i.e. RHEL, Windows 2003 etc.		
7.2.2	Operating System of Application Server with Version i.e. RHEL, Windows 2003 etc.		

7.2.3	Operating System of Data Base Server with Version i.e. RHEL, Windows 2003 etc.			
7.2.4	Operating System of Any Other Server with Version i.e. RHEL, Windows 2003 etc.			
7. 3	**Other Software requirements for hosting**			
7.3.1	Web Server Software with Version i.e. Apache, IIS etc.			
7.3.2	Application Server with version i.e. Tomcat, JBOSS etc.			
7.3.3	Data Base Server required with version i.e. Oracle 10g, SQL-2005 etc.			
7.4	**Integration with Other Software systems required**			
7.4.1	Specify details of the Software i.e. DMS / GIS /SMS gateway etc.			
8	**e-Mail Account required on mail.rajasthan.gov.in mail server** *(for admin)* **Remarks**			
8.1	Web Based Mail Access required	Yes [ ]	No [ ]	
8.2	IMAP/PoP3 service required	Yes [ ]	No [ ]	
8.3	SMTP service required			
8.4	Number of e-Mail Address required on State Mail Server.			Specify list of e-mail addresses to be created i.e. xyz@rajasthan.gov.in
8.5	Per User Mail Box quota required in Mb (Default 50MB)			
9	**FTP Access required in demilitarized zone**			
9.1	FTP access required over Internet	Yes [ ]	No [ ]	If yes Provide real IP
9.2	Proposed FTP User Name demanded by the department			

10	**Other Requirements**			
10.1	SSL Certificate (VeriSign) Required	Yes [ ]	No [ ]	
10.2	Digital Signatures Required	Yes [ ]	No [ ]	
10.3	Details of Server Port no. to be used			
11	**Safe to Host Certificate Details**			
11.1	Name of Certifying Agency			
11.2	Certificate issue date			
11.3	Certificate Enclosed Y/N			
11.4	Expiry of Certificate			

Note:

1. ***Any kind of hardware at SDC will be provided on a shared basis if not mentioned as dedicated.***
2. ***Please also attach required configuration of application software (IIS/apache/Jboss / Webshpare / Weblogic etc).***
3. ***Application developer is responsible for first time installation.***
4. ***Application developer will provide complete work flow / data flow of application in the form of solution document for future installation.***
5. ***Application fine tuning is sole responsibility of application developer.***
6. ***In case of SI/large project re-installation will be the responsibility of SI.***
7. ***Load testing report .***

Checklist for Secure Code Programming in Applications

S.No.	Action Item(s)	Is implemented?
1	Implement CAPTCHA on all entry-forms in PUBLIC pages. Implement CAPTCHA or account-lockout feature on the login form. [Alpha-numeric CAPTCHA with minimum 6 characters]	□YES □NO □Not Applicable
2	Implement proper validations on all input parameters in client and server side (both). [White-listing of characters is preferred over Black-listing]	□YES □NO □Not Applicable
3	Use parameterized queries or Stored-procedures to query output from databases, instead of inline SQL queries [Prevention of SQL Injection]	□YES □NO □Not Applicable
4	Implement proper Audit/Action Trails in applications	□YES □NO □Not Applicable
5	Use different Pre and Post authentication session-values/Authentication-cookies	□YES □NO □Not Applicable
6	Implement proper Access matrix (Access Control List-ACL) to prevent un-authorized access to resources/pages/forms in website [Prevention of Privilege escalation and restrict in of access to authorized/authenticated content]	□YES □NO □Not Applicable
7	Do not reference components (such as javascripts,stylesheets etc.) directly third-party sites. [They may be downloaded and self-referenced in website]	□YES □NO □Not Applicable
8	Use third-Party components from trusted source only. [Components with known vulnerabilities are not recommended.]	□YES □NO □Not Applicable
9	Store critical data such as PAN number,Mobile Number,Aadhar Card number etc. in encrypted form in the database. [Hashing of sensitive information is preferred over encryption, unless required to be decrypted]	□YES □NO □Not Applicable
10	Prevent critical information from public access by any mean [Critical information like credit card number, account number, aadhar number etc. should be restricted to authorized persons only. If such information is stored in static files such as excel,pdf etc., sufficient measures should be taken so that is it not accessible to unauthorized persons or in public.]	□YES □NO □Not Applicable
11	Hash the password before it is relayed over network, or is stored in database. [During login, password should be salt-hashed using SHA-256/512. However, it should be stored as plain hash (SHA-256/512) in database. On every login attempt, new salt should be used, and it should be generated from server-side only]	□YES □NO □Not Applicable
12	Implement Change Password and Forgot password module in applications [not required in applications, using LDAP for authentication]	□YES □NO □Not Applicable
13	Comply with Password Policy, wherever passwords are being used.	□YES □NO □Not Applicable
14	Use Post methods to pass parameters as values from one-page/website to another. [GET methods should be avoided]	□YES □NO □Not Applicable
15	Implement proper error-handling. [System/application errors should not be displayed to viewer]	□YES □NO □Not Applicable

16	Implement token-based system that changes on every web-request in application, to prevent CSRF. [CSRF Guard or Anti-forgery tokens can be implemented in non-critical applications. Websites using payment-gateways etc. are categorized in critical websites.]	□YES □NO □Not Applicable
17	Do not implement File upload in public modules	□YES □NO □ Not Applicable
18	Store uploaded files in database, rather than storing them in file-system [Files, stored in database cannot be executed directly, hence this is more secure than storing them in file system.]	□YES □NO □Not Applicable
19	Generate unique, un-predictable and non-sequential receipt numbers/acknowledgement numbers/application numbers/roll numbers/ File-names etc. It is preferable that strong algorithm be used to generate such numbers.	□YES □NO □Not Applicable
20	Implement proper Session Timeout [Logged-In user should be logged-out after a specific period(say 20 minutes) of inactivity]	□YES □NO □Not Applicable
21	Assure admin/Super-Admin URL's is/are accessible from restricted IP's only [For this, segregate public URL from Admin/Super-Admin module. Public modules and Admin/Super-Admin modules should be deployed on separate URL's. Admin/Super-Admin URL's should be accessible from restricted IP's only. It is preferable to allow access for Admin/Super-Admin modules through VPN]	□YES □NO □Not Applicable
Other Action Item(s)		
1	Assure third-Party links/page(partial/full) open in different tab, with a disclaimer.	□YES □NO □Not Applicable
2	Disable Trace/PUT/DELETE and other non-required methods in application/web-server.	□YES □NO □Not Applicable
3	Assure that Email addresses, where ever used, are in form of an image. [Alternatively, replace "@" with [at] and "." with [dot] in email addresses]	□YES □NO □Not Applicable
4	Disable directory listing	□YES □NO □Not Applicable
5	Set "Auto Complete" off for textboxes in forms	□YES □NO □Not Applicable
6	Prevent pages from being stored in history/cache. [Each time that the user tries to fetch a page, it should request server to serve with a fresh copy of the page]	□YES □NO □Not Applicable
7	Implement Logout buttons in all authenticated pages	□YES □NO □Not Applicable
Implementation Guidelines		
1	Restrict each application for minimum access (only required access) [Allow access of application for restricted network access. Websites, those are to be used in local-network, should not be accessible from any other network. For exceptional cases, VPN may be used. Websites, those are required to be accessed from within the country, should be restricted for access on Indian ISP's ONLY.]	□YES □NO □Not Applicable
2	Use the latest and non-vulnerable versions of Application Server (IIS/Apache etc.), Jqueryetc.	□YES □NO □Not Applicable
3	Enable audit-trails and system logs on server [e.g. :Web-Access logs, Application Logs, Security Logs etc.	

4	Take regular backups of data and application [Sufficient arrangements should be made to take proper and regular backups of database,application and other related objects/components, for retrieval on undesirable circumstances. It is preferable to maintain a set of last 5 backups. It is advised to store backups on hard-drive/tape-disks/SAN-storage. Networked servers/machines should be avoided for this activity]	□ YES □ NO □ Not Applicable

For detailed checklist for developers and secure codingguidelines, visit: https://security.nic.in/appsec_new.aspx?pid=114&id=118&index=2

Seal & Sign of the Project OIC (DoIT&C/RISL) / SA (Joint Director) / ACP (Deputy Director) / Technical Partner for the Project

Department / Organization :

Place :