Referral Guidelines for Development of Websites Of Government of Rajasthan

April-2021

AdoptedBy,
Department of Information Technology & Communications, Government of Rajasthan,
Ist Floor, Yojana Bhawan, Tilak
Marg, C-Scheme, Jaipur.

Based on Contents Developedby,
National Informatics Center,
Department of Information Technology
Ministry of Communications and Information Technology, Government of India.
http://web.guidelines.gov.in/

(1) INTRODUCTION

(a) BACKGROUND

As the Internet is gradually transforming the social and economic fabric of our communities, Government of Rajasthan is committed to deploy IT as an effective tool for catalyzing accelerated economic growth, efficient governance and human resource development. Web Sites and Portals have emerged as the logical front end for government initiatives to deliver a wide variety of information and services to its citizens. Wherever citizen interface is involved, Web enabled applications will be developed.

Since the website of a department is its reflection to the outside world, it ought to be seen as an integral part of the Department, rather than an external entity. Hence all facets of the department and its activities should be appropriately reflected on the website. All public domain information like official gazette notifications, acts, rules, regulations, circulars, policies and programmed documents should be digitized and made available for electronic access on Web. However, many of websites belonging to the departments, boards, corporations and its subordinate's offices etc., have already been operational. But many websites follows different technology standards, design layouts, navigations, transitions, different look & feel and some websites are not mobile compatible. This is resulting in lot of inconvenience to citizen, as he/she needs to interact with the functionality of each individual website, in different way. Common look and feel in Government websites helps in promoting the brand image of the Government; raises user confidence; provides a user-friendly experience in navigating Government websites; and organizes information more consistently to facilitate search.

(b) SCOPE & OBJECTIVE

The entire effort of developing and hosting websites of different Departments, Boards & Corporations needs to streamlined and integrated. To achieve this, it is important to have common guidelines and policy for the Website Development, Hosting and Maintenance for various State Government Departments, Boards and Corporations. This guideline document address common policy issues and practical challenges that Government Department face during development and management of their websites. The aim of this guideline is to assist the departments in ensuring that their websites conform to a consistently required standard. This will show the uniformity in all websites belonging to Government Departments and citizen will not have to familiarize himself/herself with the functionality of each individual website.

(c) COMPLIANCE TO GUIDELINES

This guideline document complies to all International Standards including ISO/IEC/IEEE 23026-2015, W3C's, Web Content Accessibility Guidelines (WCAG 2.1), GIGW 2.0, Disability Act of India, Data Protection bill and IT Act of India.

(d) **APPLICABILITY**

All the websites of the Departments, Boards and Corporations of the Government of Rajasthan and their subordinate and attached offices have to **ensure compliance of latest GIGW 2.0 guidelines**issued by Govt. of India available at http://web.guidelines.gov.in. A referral guideline has been compiled by DoIT&C, Govt. of Rajasthan to help in the conceptualization of websites of State government departments.

Detailed information on the WCAG guidelines and the techniques for compliance can be found at the W3C website. Developers must visit the website to get information on the various success criteria related with each of the guidelines.

(2) HOSTING OF WEBSITE

(a) **DomainName**

Hence, in compliance to the Governments domain name policy, all Rajasthan Government websites must use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The above naming policy applies to all Government websites irrespective of where they are hosted. In website domain name .com & .org etc. should bemigrated in the domain stated above.

All the websites of Government of Rajasthan should be under the sub domain of rajasthan.gov.in.

The RajComp Info Services Limited, is the exclusive Registrar for rajasthan.gov.In domain names. The domain name registration form is given in Annexure-1 for registration of the domain under rajasthan.gov.In.

(b) **Site ofHosting**

The websites/portals/web applications should be accessible on internet. The websites/portals/ web application should be accessible and available 24*7 to the visitors. For ensure the 24*7 availability of websites/portals/web applications a high end infrastructure is required, that consists the large number of servers, storage system with storage area network, a high speed networking infrastructure, 24*7 power supply, backup and multi-tier security system.

The Rajasthan Government has its own data center with Tier-3 & Tier-4 category situated at Yojna Bhawan (RSDC-Phase-III), Jaipur and Rajasthan State Data Center Phase-IV, Jhalana institutional area, Jaipur respectively. Both data centers are equipped with required high end infrastructure with disaster recovery site situated in Jodhpur. Both data center follows the international standard for high end security. As per mandate RSDC Phase-IV would be the production site and RSDC Phase-III would be near

DR Site.

As Government websites/portals/web application contains the information about the Government, it is MANDATORY for all Government Department to host their websites/portals/web applications at Rajasthan State Data Center Phase-IV, Jhalana institutional area Jaipur.

To host the Website at Rajasthan State Data Center (RSDC) letter may be sent by Head of the Department to DoIT&C along with duly filled "Requisition for Application/Website/Domain Hosting" form attached as Annexure-I.

(c) **OwnershipControl**

The ownership regarding content, information and application business rules remains with the department/organization/person having the Administrative and Signatory rights i.e. the host Department. However, the technical control with regards to problems in Web server on which the site ishosted remains with the agency maintaining the Web Server.

(d) **Content Responsibility**

The web content is entirely different from that of the print and audiovisual mediaand needs special care for drafting. The web content can serve multiple purposes and can be both brief as well as detailed. The details about the content is provided in Content section of this document. All Government entities should comply the guideline for content management as provided in this document.

The responsibility of contents published on website lies with the ownerdepartment.

(e) **SecurityAudit**

Web security is most important aspect that need to be taken care during the development. POIC must ensure white box testing during the development and change management.To ensure the security of website/portal/web-application, periodicsecurity audits must be conducted. As per the guidelines security audit must be conducted every year, however, for major code change, it is to be conducted before moving to production environment of data center.

Best practices to follow while developing web applications using various technologies are available on CERT-IN website (http://www.cert-in.org.in). CERT-IN has empaneled a number of agencies to conduct the security audit of Websites/ Applications.

Center for Application Development (CAD) has also issued a draft "General Software Development Standard and Guidelines", which will be further refined in due course of time, should also be followed.

Each Website / application must undergo a security audittwice in a year from empaneled agencies with

CERT-IN, and clear the same, prior to hosting at the State Datacenter.

In this regard, guideline framed is annexed at annexure-VI.

(3) CONTENT OF WEBSITE

Content is most important part of any website/application it could be static and dynamic in nature. Content is a sensitive information shared in public domain through websites/applications, which keep update the visitors about the organization and its activities. Websites/applications should be regularly monitored and assessed to ensure content authentication and updation.

- The homepage of a website is the primary entry page for entire content of the website. It is important that the visitors of site get to access the most important content.Government websites/applicationsmust ensure the availability of theminimum content elements on the homepage as mentioned in annexure II and annexure III.
-

(4) WEBSITE DESIGN

The compliance checklists for development of website is provided in Annexure-IV & Annexure-V. Departments may refer the checklists to ensure the compliance of this guideline document.

(5) DISASTER RECOVERYMANAGEMENT

The website/application of a Government Department is its presence on the Internet and it is very important that the site is fully functional at all times. It is expected that Government websites/applicationsshoulddeliver information and services on 24x7 basis. Hence, all efforts should be made to minimize the downtime of the website as far as possible.

It is therefore necessary that a proper Disaster Recovery Plan for the website/applicationshould be prepared in advance to handle any eventualities and restore the site in the shortest possible time. Regular DR drill must be organized with DC and DR team.

(6) WEBSITE PROMOTION

Today rapid development of websites/applicationsare going on. Billions of websites/applications are available on internet dealing same or many subject matters. The visibility of website/applicationover the internet is very challenging. The ultimate aim of any Government website should be to provide information and services to citizens as possible. The existence of any Government website/application lying inaccessible on the web is meaningless. For this purpose a conscious and concentrated effort has to be made to increase the reach of the website by concern OIC/department.

Apart from search engines the website may be promoted through other media like print, television etc. This will prompt casual visitors to browse the website and if they find the information useful, they may visit the site more often.

(7) WEBSITE MANAGEMENT

(a) **Website Management Team –** Minimum Team required for any in-house website design and hosting comprises of:

i. Web Administrator
ii. Content Creator/ Designer
iii. Web Site Developer
iv. Graphic Designer/ UI/UX Designer/ Artist

(b) **Website Development & Maintenance Tools**-

i. **Website Authoring Tools** - Website Authoring Tool is a software for generating well-engineered web pages. Following website authoring tools available in market are as under:

a. Adobe Suite
b. XEMacs
c. Quanta Plus
d. ASAP

One can choose any tool based on the requirements, however, the following should be ensured while selecting the tool:

a. It generates pages that conform to all of the requirements, recommendations and options of this guideline.
b. It conforms to the Web Consortium's Authoring Tool Accessibility Guidelines.

ii. **Web Content Management Tools** - A web Content Management System (CMS) is the software used for creating and managing web content. It is used to manage and control a large, dynamic collection of content on a website/portal (HTML documents and their associated documents and files). CMS facilitates content creation, content control, editing, and many essential content maintenance functions.

Following are tools may be used for managing the graphical, animated and dynamic web pages content:

a. **Graphics**

- Adobe Acrobat to create PDF files for download
- Fireworks from Macromedia
- Adobe Photoshop for web graphics
- Online crunching of the gif and jpeg files

b. **Animations**

- Macromedia Flash

c. **Dynamic Web Pages**

- Adobe Suite
- Visual InterDev, Visual studio .NET
- Java Angular JS etc
- Flask/ Django(Python)
- PHP

d. **Scanning Software**

- Finereader
- OmniPage

iii. **Web Analytical Tools -** Many organizations uses different types of statistics to measure the impact of the site and also for reorganizing or enhancing their website further. Some uses simple counters, while others are using more sophisticated Web analyzer tools to obtain data. Counters add little value to a site and often appear to be self-congratulatory. Web analyzer tools provide more information and are virtually transparent to the end user, therefore, Web analyzer tools should be the standard means of collecting site usage data. Counters should not be used to perform this function.

Web Monitoring/Review and Enhancement– All Government websites/applications should have monitoring policy in place. Website/Applications must be monitored periodically in accordance with the plan to address and fix the quality, security and compatibility issues by monitoring the parameters like Performance, Functionality, Broken Links, Traffic Analysis and Feedback. On the basis ofthis monitoring report, the websites/applications should be enhanced/pached.

(c) **Administration/ Maintenance/ Updation**

i. Organization will appoint a Nodal Officer for each website who will be responsible for overall supervision to ensure that authentic and updated information is available on the website.

ii. Nodal Officer will be responsible for timely updating of the website after approval by the Department. Nodal officer must ensuretimely deletion of irrelevant and undesired information/pages.

iii. Nodal Officers deputed in the departments should compulsorily monitor, review and update the website periodically at least once a fortnight i.e. 1st and 16th of every month with the date of updating being displayed on the website each time the work is done. Subsequently a certificate should also be issued by the Nodal Officer by the 5th of every month to Information Technology & Communication Department stating that the information on the web site has been updated to reflect the position as on the 1st of that month.

iv. Content Administrator/Nodal Officer will visit the website at least twice a week to update/modify contents. Any feedback or email received through the website would be treated as an official receipt and action taken as required.

v. Where the Department has the requisite technical competency, Head of Department may authorize a suitable person for modification and uploading of content on the website after due approval.

(8) REFERENCES

a. GiGW Manual (Guideline for Indian Government Websites v2.0) : - https://web.guidelines.gov.in

b. ISO/IEC/IEEE 2026-2015 Standard - https://www.iso.org/obp

c. Web Content Accessibility Guidelines (WCAG) 2.1 : - https://www.w3.org/TR/WCAG21

d. The Personal Data Protection Bill 2018 - https://meity.gov.in

(9) ANNEXURES

a) Annexure – I

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(Ann ual Maintena ce Contract) n**	
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, Windows2003 etc.			
7.2.4	Operating System of Any Other Server withVersion i.e. RHEL, Windows2003 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. ***AnykindofhardwareatSDCwillbeprovidedonasharedbasisifnotmentionedasdedicated.***
2. ***Pleasealsoattachrequiredconfigurationofapplicationsoftware(IIS/apache/Jboss/Webshpare/ Weblogicetc).***
3. ***Applicationdeveloperisresponsibleforfirsttimeinstallation.***
4. ***Applicationdeveloperwillprovidecompleteworkflow/dataflowofapplicationintheformofsolution document for futureinstallation.***
5. ***Application developer will also provide list of all the dependencies.***
6. ***Applicationfinetuningissoleresponsibilityofapplicationdeveloper.***
7. ***IncaseofSI/largeprojectre-installationwill bethe responsibilityofSI.***
8. ***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.	☐ YES ☐NO ☐Not Applicable

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 coding guidelines, 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 theProject

Department / Organization : Place :

b) ANNEXURE – II

Checklist of a Website Contents

1. Aboutdepartment
2. DepartmentLogo
3. Organogram
4. Functions /Objectives
5. Achievements
6. Nodal Officer with contactdetails
7. Last UpdationDate
8. Photos and Names of DepartmentOfficers
9. Related department Principal Secretary / Secretary / Director contactdetails
10. Color theme of the Website (should not be toodark)
11. Important links to the related Websites
12. Proper linking of pages within and outside theWebsite
13. News, Events andSchemes
14. Documents / Forms / Tendersdownloads
15. PhotoGallery
16. Vacancy
17. Feedback
18. FAQ’s
19. RTIAct
20. Departmental Acts andRegulations

c) ANNEXURE – III

Minimum Required Content

The website/application of a Government Department / Organization must include at least the following information and facilities on their websites:

- Complete Identity of theDepartment
- Aims, Objectives &Responsibilities
- Plans, Schemes, Programs, Projects of theDepartment
- Organization Structure including Agencies, Directoratesetc.
- Generic Postal Address, Fax, Phone Number & E-mail of theDepartment
- Names and Telephone Numbers or E-mail Addresses of contacts for further information on specific policies or services
- Services offered by theDepartment
- Application Forms dealt by the Department and guidance for their completion
- Documents published by the Department
- Information related to RTI
- Submit aquery/grievance
- Legislation for which the department has the lead, or a link to a site which containsit
- Pressnotices
- Links to customized view of Directory of relatedDepartments.
- Search
- Feedback
- Sitemap

d) ANNEXURE – IV

Steps for developing a Website

1. Finalize contents: Department/ Organization should compile their own list of contents/ sub contents which they feel should be in public domain or needed by their intendedaudience.
2. Choose an agency to develop a Website: The Department can get the website developed in house if technical expertise/skills are available in the department. The website can be developed by a commercial agency with the experience of the task as per rules or get the website developed byRISL.
3. Finalize the design/Layout: The color/layout may be chosen analogous to the department and intended audience. A consistent page layout must be maintained throughout the site. This means that the placement of Menu, sub menu and buttons should be uniform across thewebsite.
4. Selecting the URL of the website: The Domain name has a lot of significance and therefore should be chosen to easily address the department like krishi.rajasthan.gov.in or agriculture.rajasthan.gov.in for Agriculture Department etc.
5. **Procurement of SSL Certificate:**Project OIC/Department will procure SSL certificate for the approved domain (in the case of new hosting) on the basis of rate contract (RC) done by Website Cell.
6. Appoint a Nodal Officer: Organization should appoint a Nodal Officer who would be responsible for overall supervision to ensure that authentic and updated informationisavailableonthewebsiteafterapprovalbytheDepartment. Timely deletion of irrelevant and undesired information will also have to be ensured by him/her.
7. Safe to host certification: Each Website / application must undergo a security audit from empaneled agencies with CERT-IN and clear the same, prior to hosting at the State Datacenter.
8. Emergency Hosting: For urgent hosting due to inauguration etc. or due to some other important event/activity, the hosting can be done by internal security audit, which is valid for six month and during this period website/application should be security audited from Cert-In empaneled agencies.
9. Vulnerability patching: Vulnerabilities found during security audit would be patched/mitigated by the developer and iteration will go on till zero vulnerability.
10. Maintenance contract for Content Management: To ensure regular Updation and modification, the maintenance contract should be made with an agency as per therules.
11. Fill the form of requisite for hosting Website : To host the site after the approval of the Department at the State Data Center , a letter may be sent by Head of Department to DOIT&C along with duly filled form “Requisition for Application/Website/Domain Hosting” atAnnexure-I.
12. Regular Updation: Nodal Officer should ensure that the updated information is available on the website.
13. Renewal of Contract: In order to ensure smooth running of the website, POIC/Department should take measures for timely renewal of thecontract, security audit and SSL Certificate.

e) **ANNEXURE – V**

Website Development Checklist

Pre-Development Phase

1. For small and medium website, AMC for the website should be 1 year from the date of acceptance / go-live.
2. Department will clearly define the milestone for making payments to the developer firm.
3. DoITC will have its own State Software repository of the successful projects and will ensure there is no duplication in efforts for website development.
4. Intellectual Property Rights(IPR) of the source code will vest solely with the Government of Rajasthan. However, such a system will not be allowed to be misused by quoting same website/portal/web application to other districts or departments.
5. Representatives of development firm working on the project must sign the Agreement with project owner of concerneddepartment.
6. Use of Standard Components such as Payment Gateway, SMS Gateway, Email, etc would be provided as per SDC RateChart.

Development Phase

1. Bilingual Menus/ Tabs on all the pages of the portal. On selecting the language at the home/index page, language of menus/ tabs at all the pages shall change to selected language.
2. Website/Application should be developed with rajasthan.gov.inextension.
3. Website/Application should run independent of IP Address. i.e. IP Addresses should be not be hard coded in the sourcecode/configuration.
4. Website/Application should be IPv6compliant.
5. Website/Application should be able to open in all six ways. Forexample,
   - https://www.rajasthan.gov.in
   - http://www.rajasthan.gov.in
   - www.rajasthan.gov.in
   - https://rajasthan.gov.in
   - http://rajasthan.gov.in
   - rajasthan.gov.in
6. Website/Application should be running on SSL i.e. http request should automatically get redirected tohttps
7. Website/Application should be compatible to run on multi server environment for loadsharing
8. Website/Application should be compatible for accessibility from any device, any Operating System and any browser.
9. Website/Application must be responsive on
   - All mobiles above 4” Screen Size
   - All tablets, including iPad
   - All primary desktop and laptop screen resolution

10. All GoR (Government of Rajasthan) Web Portals/websites must support multiple language
11. The portals to be developed must comply with the following international and national guidelines:
    - W3C HTML5
    - WCAG, i.e. Web Content Accessibility Guidelines 2.0
    - UAAG, i.e. User Agent Accessibility Guidelines 2.0
    - GIGW, i.e. Guidelines for Indian Government Portals
12. Bidder shall incorporate Security features as per latest OWASP Top 10 vulnerabilities.
13. Developed in Three (3) different themes where in colours of tabs, and other background User Interface (UI) can be changed with minimal efforts
14. Functionality to add and remove tabs/ menus in the web pages by the admin of the portal
15. Different Access Levels on the developed portal for closed user groups
16. Facility for maintaining number of visits to the portal
17. Module for uploading, editing of nodal officer details of the developed website/application
18. Search functionality to search the portal for any content etc. with advance search
19. Functionality for increasing / decreasing the fonts on the website/application
20. Print, Bookmark, Emails, Conversion to printable PDF format available on each page
21. Tooltips for icons displayed on mouse over.
22. Platform used for Website such as OS, DB, Java, etc. software should be N-1 where N is the latest version prevailing.
23. CAPTCHA should be present for web pages with form field such as feedback form, registration form etc.
24. Password policy of State must be enforced and passwords should not be hardcoded in any website/application, pages and configuration files and should not be stored as plain text in database.
25. Application login logs must be maintained.
26. File upload utility should be avoided; if necessary, than, this module should have strict authentication mechanism and also have strict file size and type restrictions.

Post-Development Phase

1. Level 0 check to be complied by the developer for GIGW compliance and address Top-10 vulnerabilities as per OWASP.
2. Security Audit :
    a. Security Audit shall be performed by the Cert-In empaneled Security Audit agency.
    b. If the website/applicationis proposed to be develop by outsource agency than the Security Audit clause should be part of the RFP, and the cost of security audit should be borne by the developer. If the application is proposed under maintenance phase, than on major code change and periodic (i.e. annual/bi-annual as the case may be) security audit must be the responsibility of developer agency.
    c. For any reason, under emergency hosting, internal security audit would be done which is valid for six month and during this period POIC/Department should be the responsible to get the security audit certificate from emplaned agency.

d. Vulnerabilities found during security audit would be patched/mitigated by the developer and the iteration will go on tell zero vulnerability.

3. Security Audit Certificate to be mandated along with Hash5 code. Source code along with Hash5 code of the website/application to be submitted by Developer. Documentation of Source Code along with Administration/User Manuals needs to be submitted.
4. DoITC would also facilitate the checks for GIGW compliance and Accessibility of the website/application.
5. The project will be treated as "complete" only if:
   - UAT is completed
   - Handover to the Department is completed
   - Website/Application is hosted on the RSDC and GoLive.
   - Final Source code along with Security Audit Certificate (with Hash5) of the project along with detailed documentation and IPR is being transferred to DoITC for State Software Repository.
6. It is advisable to host the Website/Application in the Rajasthan State Data Centre for which below compliance needs to be adhered. To get the security audit carried out, below process needs to be followed:
   - Details of the website/application such as Operating System, Database used, Web Servers used, Data Storage required, etc. needs to be provided to DoIT for due scrutiny.
   - After due scrutiny of the details provided to start the audit process, developer needs to visit RSDC for making site available in staging area.
   - Security Auditor would perform Level-1 Audit of the website/application. After Level-1 audit completion, if any vulnerability found then developer needs to rectify and revert to security audit team for further checking. This process will be repeated until known vulnerabilities gets rectified.
   - Security audit Certificate will get issued by security audit agency & a copy will be provided to the concerned department.
   - Department/developer will copy the audited code to the production environment. POIC will issue a certificate that the provide code is the same on which security audit has completed and no additional code/ pages are included after audit. He will install SSL certificate on production server. Developer will ensure port redirection from port 80 to 443.
   - Department/POIC will fill change request form(CRF) for port opening (port 80 & 443 or as per requirement of the project). This will be taken as standard request. All email communication will be accepted only from government email ids.

f) ANNEXURE – VI

Given below is a checklist of mandatory guidelines outlined in this document. Departments may use this checklist to validate their websites against these guidelines and make necessary modification to ensure compliance.

COMPLIANCE MATRIX of GIGW		
Websites - General Guidelines		
S.No.	**GUIDELINE**	**Yes/No**
1	Department has nominated a Web Information Manager as defined in the guidelines.	
2	It has been ensured that all stationery of the department as well as advertisements/public messages issued by the concerned Department prominently display the URL of the web site.	
3	Website has the following clearly defined policies and plans approved by the web information manager.	
	1. Copyright Policy.	
	2. Content Contribution, Moderation & Approval (CMAP) policy.	
	3. Content Archival (CAP) policy.	
	4. Content Review (CRP) policy.	
	5. Hyper linking Policy.	
	6. Privacy Policy.	
	7. Terms & Conditions.	
	8. Website Monitoring Plan.	
	9. Contingency Management Plan.	
	10. Security Policy.	
4	Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned.	
5	Due permissions have been obtained for publishing any content protected by copyright.	
6	Home page of website displays the last updated/reviewed date.	
7	Complete information including title, size format and usage instructions is provided for all downloadable material.	
8	With respect to each, Circular, Notification, Document,	
	Form, Scheme, Service and Recruitment notice,	
	The following should be clearly listed in the Website:	
	a. Complete title	
	b. Language (if other than English)	
	d. Purpose/procedure to apply (as applicable)	
	e. Validity (if applicable)	

9	All outdated, irrelevant content (like Announcements, Tenders, Recruitment notices, News and Press Releases) is removed from the website and/or placed into the archives as per the archival policy.	
10	The language is free from spelling and grammatical errors.	
11	Mechanism is in place to ensure that there are no ‘broken links’ (internal as well as external) or ‘Page not found’ errors.	
12	There are no links to ‘under construction’ pages.	
13	The mechanism is in place to check the accuracy of Hyperlinked Content and Clear indications are given when a link leads out to a non government website.	
14	Website provides a prominent link to the ‘National Portal’ from the Home Page and Pages belonging to National Portal load in new browser window.	
15	Association to Government is demonstrated by the use of Emblem/Logo in proper ratio and color, prominently displayed on the homepage of the website.	
16	Ownership information is displayed on the homepage and on all important entry pages of the website and each subsequent page is a standalone entity in terms of ownership, navigation and context of content.	
17	Website uses Cascading Style Sheets to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes.	
18	Website is readable even when style sheets are switched off or not loaded.	
19	Proper page title and language attribute along with metadata for page like keywords and description are appropriately included.	
20	Data tables have been provided with necessary tags/markup.	
21	The website has a readily available Help section linked from all pages of the website.	
22	All information about the department, useful for the citizen and other stakeholders, is present in the ‘About Us’ section and mechanism is in place to keep the information up to date.	
23	Website has a ‘Contact Us’ page providing complete contact details of important functionaries in the department and this is linked from the Home Page and all relevant places in the website.	
24	Feedback is collected through online forms and mechanism is in place to ensure timely response to feedback/queries received through the website.	
25	The website has been tested on multiple browsers. Hindi/Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout).	
26	Minimum content as prescribed in the guidelines is present on the homepage and all subsequent pages.	
27	It is ensured through content moderation and approval policy that Website content is free from offensive/discriminatory language.	
28	Text is readable both in electronic and print format and the content prints correctly on an A4 size paper.	
29	Website has cleared security audit.	
30	Website is in the nic.in or gov.in domain.	
31	Website is hosted in a data centre in india having the following facilities:	

	1. State-of-the art multi-tier security infrastructure as well as devices such as firewall and intrusion prevention systems.	
	2. Redundant server infrastructure for high availability.	
	3. Disaster Recovery (DR) Centre in a geographically distant location.	
	4. Helpdesk & technical support on 24x7x365 basis.	
32	Website is bilingual with a prominent language selection link and uses Unicode characters.	
33	Documents/Pages in multiple languages are updated simultaneously.	
34	Documents are provided either in HTML or other accessible formats. Download details (File Format Size) & instruction for viewing these is provided.	
35	Mechanism is in place to ensure that all tender/recruitment notices are published/linked through the website.	
36	All documents have a publish date on the main page.	

Websites - Accessibility Guidelines

S.No.	GUIDELINE	Yes/No
1	All non-text content (like images) has a text alternative that provides equivalent information as the image itself.	
2	Scanned Images of text have not been used.	
3	The visual presentation of text and images of text has a contrast ratio of at least 4.5:1 between the foreground and background. Large scale text and images of text have a contrast ratio of 3:1.	
4	Text can be resized without assistive technology up to 200 percent without loss of content or functionality.	
5	There is a mechanism to pause, stop or hide scrolling, blinking or auto updating content that starts automatically and lasts for more than 5 seconds.	
6	Web pages do not contain any content that flashes for more than three times in a second.	
7	Instructions provided for understanding and operating content do not rely solely on sensory characteristics such as shape, size, visual location, orientation, or sound.	
8	Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	
9	Captions or transcript are provided for all prerecorded and live audio and video content.	
10	For any audio on a Web page that plays automatically for more than 3 seconds, a mechanism is available to pause, stop or control the volume of the audio independently by from system volume level.	
11	Information, structure, and relationships that are conveyed visually on a web page must also be programmatically determined or are available in text.	
12	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	

13	All functionality that is available on the web page is operable through keyboard.	
14	Complete web page is navigable using keyboard only (using tab or arrow keys).	
15	Current navigation location (Keyboard focus indicator) is visible on the webpage while operating or navigating the page through a keyboard.	
16	Web pages allow the user to bypass blocks of content like navigation menus that are repeated on multiple pages (by using the skip to content link).	
17	Any web page within the website is locatable either through “search” or a “sitemap”.	
18	Navigational mechanisms that are repeated across the website occur in the same relative order on each page.	
19	If a webpage can be navigated sequentially and the navigation sequence affect the meaning of operation, then all components must receive focus in the same meaningful sequence (Creating a logical tab order through links, form controls, and objects).	
20	The purpose of each link is clear.	
21	Time limit for time dependent web functions is adjustable by the user.	
22	Complete & self-explanatory title that describes the topic and purpose of the page has been provided.	
23	Headings wherever used, correctly describe topic or purpose of content.	
24	Language of the complete web page has been indicated. If there is a change in language within a webpage it also indicated.	
25	Nomenclature of components that have the same functionality is uniform across the website.	
26	When any component on the web page receives focus or its settings are changed it does not initiate change in context.	
27	Changing the setting of any user interface components does not automatically cause a change in context.	
28	If an input error is detected, the item is identified and the error is described to the user in text. Suggestions for correction if known are provided to the user.	
29	Labels or instructions have been provided wherever input from the users is required.	
30	For Web pages that cause legal commitments or financial transactions a mechanism is available for reviewing, confirming, and correcting information before finalizing the submission.	
31	Web Page uses markup language as per specification.	
32	Name and Role of all interface components can be programmatically determined.	