सत्यमेव जयते

GIGW

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES

COMPLIANCE & CERTIFICATION HANDBOOK

TABLE OF CONTENTS

1. ABOUT THE DOCUMENT

About the Document | 1.0

With the launch of GIGW Manual 3.0, the Compliance & Certification Handbook too has been updated to further enhance the compliance process for Indian Government websites. As the world increasingly adopts the Internet as a medium for information and service delivery, with remarkable speed, it becomes crucial to establish robust standards that offer guidance for the development of virtual platforms. To fulfil this requirement, the Compliance & Certification Handbook has been developed by the National Informatics Center (NIC) of the Government of India.

The Guidelines for Indian Government Websites (GIGW), devised by NIC, have already become an integral part of the Central Secretariat Manual of Office Procedure (CSMOP) and have been adopted by the Department of Administrative Reforms and Public Grievances (DARPG). The Compliance & Certification Handbook serves as a complementary resource to the GIGW manual, consolidating all the relevant information in a single, easily accessible document.

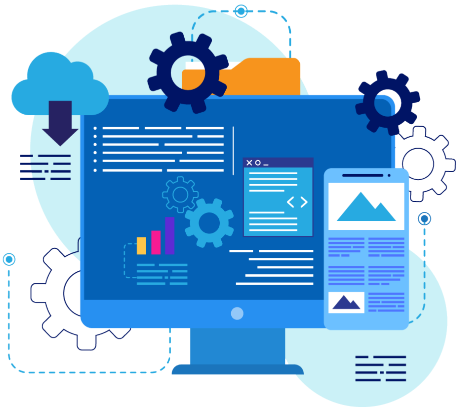
The purpose of this handbook is to assist stakeholders of Government websites in ensuring compliance with GIGW. It serves as a comprehensive reference guide, offering clear insights into various aspects that contribute to GIGW compliance. By providing a centralized source of information, the handbook simplifies the process of understanding the requirements and aids in completing the certification process.

To support the implementation of GIGW and the usage of this handbook, registered users can access the manual on the website http://guidelines.gov.in. Additionally, a dedicated helpdesk is available during office hours on all working days to address any queries or concerns. Furthermore, the NIC conducts regular workshops to further facilitate the compliance journey for Indian Government websites.

By adhering to the Compliance & Certification Handbook, government websites can ensure they meet the necessary standards and provide an optimal experience to users. This document is an indispensable tool for all stakeholders involved in the development, maintenance, and oversight of Government websites, empowering them to effectively navigate the GIGW compliance process and achieve successful certification.

2. BACKGROUND

Background | 2.0



India's digital transformation has had a profound impact on every aspect of life, ensuring that everyone has access to digital resources and services. This journey is based on sustainable, affordable, and transformative technology, and the Digital India program has driven the adoption of advanced technologies by government entities throughout the country. We are fully committed to achieving our goal of a $5 trillion inclusive digital economy, which provides opportunities for all.

The future of technology will be unlike anything we have experienced before. The use of emerging technologies such as Artificial Intelligence, Machine Learning, Extended Reality/Augmented Reality, and High-Power compute will drive innovation in various fields.

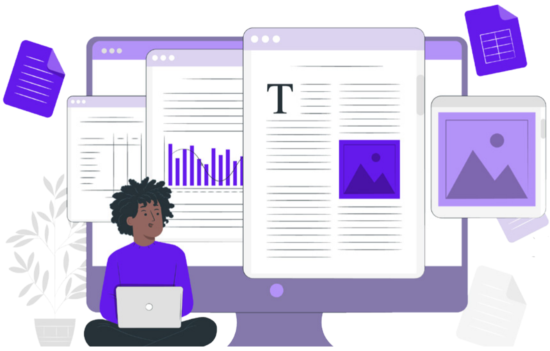
As the digital realm continues to play a larger and more influential role in our daily lives, it is essential to establish guidelines that facilitate navigation for all citizens. Website stakeholders need to consider the human-computer interface, ensuring that all individuals, including those with different abilities, can access and benefit from digital platforms. To draw an analogy, just as multi-story buildings have elevators in addition to staircases to enable accessibility for people with limited mobility, websites should provide accessible features for citizens with different abilities. For instance, a government website can offer a text transcript of an audio file, allowing audio-impaired individuals to read the information or utilize assistive technologies like screen readers for visually challenged citizens. By implementing these simple yet significant measures, the government demonstrates its commitment to meeting the needs of all citizens and promoting inclusivity in governance, regardless of their abilities, bandwidth access, or technological resources.

To establish a minimum standard for all government websites, the National Informatics Centre (NIC) formulated the “Guidelines for Indian Government Websites” (GIGW). These guidelines, which prioritize user-centric, user-friendly, and universally accessible websites, were adopted by the Department of Administrative Reform and Public Grievances (DARPG) and integrated into the Central Secretariat Manual of Office Procedure (CSMOP) in January 2009. The second version of GIGW (GIGW 2.0) was developed in 2019, and the current version, GIGW 3.0, is a collaborative effort between the NIC, the Standardisation Testing and Quality Certification (STQC) Directorate of the Ministry of Electronics and Information Technology, and the Indian Computer Emergency Response Team (CERT-In). This joint formulation ensures that the expertise of STQC Directorate auditors in conformity with GIGW and the cybersecurity experience and knowledge of CERT-In contribute to the guidelines.

3. WHAT IS CONFORMANCE with GIGW

What is Conformance with GIGW | 3.0

Conformance with GIGW ensures a high degree of consistency and uniformity in the content coverage, presentation security and accessibility and promotes excellence in government solutions in the Indian web space.



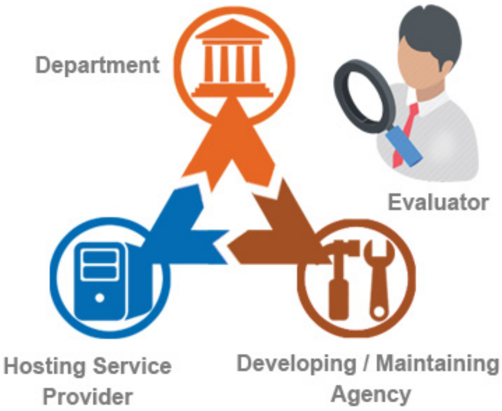
GIGW guidelines are based on international standards, including ISO 23026, W3C's Web Content Accessibility Guidelines (WCAG 2.1) Rights of Persons with Disabilities Act, 2016, as well as the Information Technology Act, 2000. Further, the long-standing experience of the authors in the design, development and management of government websites/ apps as well as their knowledge of the ground realities and challenges faced by government organisations in developing and managing their websites/apps, have helped significantly in drafting these guidelines. These guidelines also form the basis for obtaining the Website Quality Certification from the STQC Directorate. Details of the certification scheme are available at https://www.stqc.gov.in/website-quality-certification-0.

The primary emphasis of GIGW 3.0 guidelines lies in ensuring quality, accessibility, security, and life cycle management of websites. Through a comprehensive set of 88 guidelines, it offers clear explanations regarding the benefits of each guideline and the necessary actions that organizations, developers, and evaluators should undertake. Furthermore, these guidelines include references to external resources as needed. Additionally, each guideline provides information on risk factors associated with them and suggests ways to mitigate those risks.

4. ROLES & RESPONSIBILITIES OF WEBSITE STAKEHOLDERS

Roles & Responsibilities of Website Stakeholders | 4.0

The GIGW 3.0 identified three stakeholders i.e., 1) Government Organisation/ Departments 2) Developer, and 3) Evaluator for making Indian government websites/apps user-centric, more user-friendly and secure. In addition to that there is another stakeholder, though not separately identified in the GIGW 3.0, is Hosting Service Provider (HSP).



In the GIGW 3.0, recommended policies and guidelines have been provided under four sections namely Quality, Accessibility, Cybersecurity and Life Cycle Management requirements. Under each section, compliance points have been specified along with the actions required to be taken by the Government Organisation, Developer and Evaluator. HSP related action points are also included as a part of department and developer actions given in the GIGW 3.0. The concerned stakeholder is required to implement/use those action points for ensuring/assessing compliance.

Department

Department | 4.1

Department is the owner of the website, responsible for initiating design, content creation, review, modification, archiving etc. and managing operations through website lifecycle, with the help of other stakeholders like development agency & hosting service provider.

A Government department can initiate steps towards GIGW compliance by designating a Web Information Manager (WIM), at the level of Joint Secretary, who spearheads the department's website initiative. A WIM is responsible for deliverables such as:

- Approving all policies to handle legal aspects such as copyright, hyperlinking, privacy etc.
- Approving all policies for effective management of the website's content, as required by GIGW: content moderation, review, and archival.
- Approving processes and plans to effectively monitor the website and handle any contingencies.
- Ensuring effective promotion of the department's website.

Developing/ Maintaining Agency | 4.2

Development Agencies act as per the mandate from the Government department, and contribute technical expertise to design, develop & maintain department websites.

The department can engage the services of a Developing / maintaining agency to ensure the department website is developed to comply with GIGW guidelines not just at the time of website launch, but through the life of the website in the listed ways:

- All content is universally accessible
- Government identity and the department's lineage is prominently displayed through the proper use of emblem, flag etc.

- Prescribed minimum content and functionality as stipulated by GIGW is present on the website e.g., Feedback, Help, Search, Sitemap etc.

Hosting Service Provider | 4.3

Hosting Service Providers offer hosting services to ensure secure, reliable, robust availability of Government department websites.

The Hosting Service Provider can ensure GIGW compliance by providing infrastructure to enable:

- Multi-tier security
- Effective & regular backups
- Disaster recovery

Collective efforts of all stakeholders to fulfill their respective responsibilities can help deliver the desired common goal: websites that truly serve the interests of all visitors!

Refer Appendix i - Achieving GIGW Compliance using a Content Management System (CMS) to see how a Content Management System (CMS) can help comply with GIGW guidelines specific to Accessibility, Content Scope and Quality, Visual Identity, Consistent page layouts design etc.

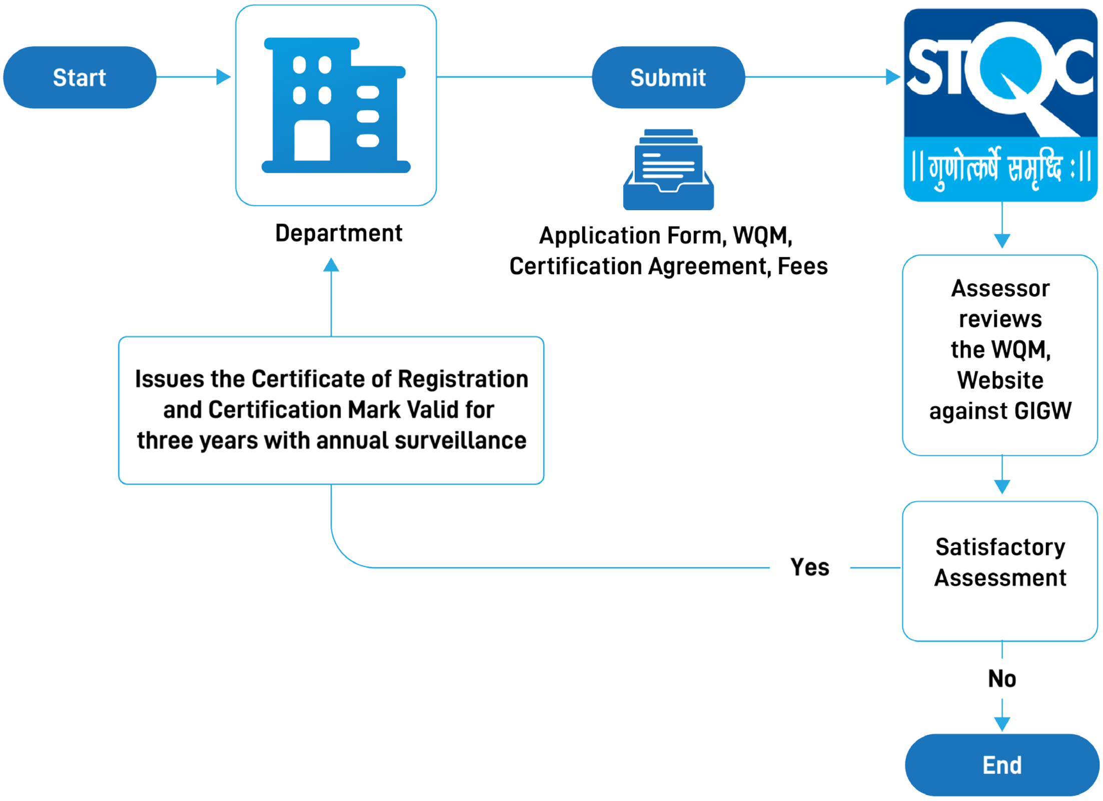
Government Departments need to prepare a Website Quality Manual (WQM) document in the predefined format attached in Appendix ii. In order to get the GIGW certification under the Website Quality Certification (WQC) scheme of STQC, the department needs to submit the WQM along with the application form and certification agreement to the STQC Certification Body. The Application form and Certification agreement formats are available at STQC official website (https://www.stqc.gov.in/).

Evaluator | 4.4

Evaluators perform assessment of websites to check the compliance as per GIGW 3.0. The assessment is carried out by:

- Document Review of Website Quality Manual (WQM), Security Certificate & Report
- Website testing
- Audit of backend processes defined in WQM

The process flow chart for obtaining GIGW certification from STQC is given below:


Start
Department
Submit
Application Form, WQM, Certification Agreement, Fees
STQC
|| गुणोत्कर्षे समृद्धि :||
Assessor reviews the WQM, Website against GIGW
Satisfactory Assessment
Yes
Issues the Certificate of Registration and Certification Mark Valid for three years with annual surveillance
No
End

5. POLICY TEMPLATES FOR STQC CERTIFICATION

5.4.3a. Copyright Policy

5.4.3b. Content Contribution, Moderation & Approval (CMAP) policy

5.4.3c. Content Archival (CAP) policy

5.4.3d. Content Review (CRP) policy

5.4.3e. Hyper linking Policy

5.4.3f. Terms & Conditions

5.4.3g. Website Monitoring Plan

5.4.3h. Privacy Policy

5.4.3i. Contingency Management Plan

5.4.3j. Security Policy

5.4.3k. Validation & Testing Process

Policy Templates for STQC Certification | 5.4.3

To keep delivering government information and services with consistently good quality through a department's website, while continually conforming to GIGW guidelines, it is important to establish a framework of "ground rules" that can be clearly understood & honored by all website stakeholders in both the design and daily operations of the website. These ground rules consider all factors that may impact the website content's accuracy, its validity, accessibility, website security, up-time etc. To enable all government website stakeholders to adopt a consistent and tested framework, so that uniformity can be maintained, a set of template policies has been devised. These templates can be suitably customized to reflect specific details of each website. Conformance in letter and spirit to these policies included in the handbook would ensure that the website meets the citizen expectation at all times: authentic, accurate, easily accessible information from a credible source such as an official Government website.

Copyright Policy | 5.4.3a

Purpose

Copyright is a form of protection provided under law to the owners of “original works of authorship” in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website.

However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

Copyright policy Moderate

Material featured on this <Website / Portal / Web Application> may be reproduced free of charge after taking proper permission by sending a mail to us. However, the material has to be reproduced accurately and not to be used in a derogatory manner or in a misleading context. Wherever the material is being published or issued to others, the source must be prominently acknowledged.

Moderate

However, the permission to reproduce this material shall not extend to any material which is identified as being copyright of a third party. Authorisation to reproduce such material must be obtained from the departments/ copyright holders concerned.

These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the exclusive jurisdiction of the courts of India.

Copyright policy Conservative

Conservative

Material featured on this <Website / Portal / Web Application> may NOT be reproduced under any circumstances.

These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the exclusive jurisdiction of the courts of India.

Copyright policy Liberal

Liberal

Material featured on this <Website / Portal / Web Application> may be reproduced free of charge. However, the material has to be reproduced accurately and not to be used in a derogatory manner or in a misleading context. Wherever the material is being published or issued to others, the source must be prominently acknowledged. However, the permission to reproduce this material shall not extend to any material which is identified as being copyright of a third party. Authorisation to reproduce such material must be obtained from the departments/copyright holders concerned.

Content Contribution, Moderation & Approval (CMAP) policy | 5.4.3b

Purpose

Each and every bit of content published on a Government website should be verified and checked thoroughly as the public expects nothing less than authentic and accurate information from a credible source such as an official Government website.

The Departments MUST have a Content Contribution, Moderation and Approval Policy (CMAP) stating the responsibility, authorisation and workflow details with regard to content publishing on the site.

Scope

- Departments/Agencies must have a (documented) process and audit trail to ensure that content has an appropriate authorization from within the Department/Agency before being published to the website.

- The documentation at minimum must show who has the authority to approve content and track the approval for each content item (showing who approved and when).

- Depending on the scale of a website, a suitable Content Contribution, Moderation and Approval Policy (CMAP) structure may be adopted.

This can be implemented easily by assigning workflow roles in the Content Management System.

Content Contribution, Moderation & Approval Policy Policy Statement for 2-tiered CMAP structure (for small websites)

The <Website / Portal / Web Application> of <Name of Ministry / Department / Organization> represents a single department where most content is contributed by a single set of sources. We hereby adopt a 2-tiered structure to implement CMAP requiring minimum 2 officials to execute the CMAP roles, viz.,

- Contributor
- Moderator/Approver

Template to implement 2-tiered CMAP structure for small websites

SECTIONS	ROLES	
	CONTRIBUTOR	**MODERATOR & APPROVER**
Home page		
News, Press Releases, Recruitments, Tenders etc.		
Who's Who, Organization Chart, Circulars/Notifications	<Preferably Admin/ Personnel Deptt>	<Preferably HOD Admin/Personnel>
Acts, Documents, Forms, Reports etc.		

Policy Statement for 3-tiered CMAP structure (for large websites)

The <Website/Portal/Web Application> of <Name of Ministry/ Department / Organization> represents multiple divisions/departments. We hereby adopt a 3-tiered structure to implement CMAP needing minimum 3 officials to execute the CMAP roles, viz.,

- Contributor
- Moderator
- Approver

Template to implement 3-tiered CMAP structure for large websites

SECTIONS	ROLES		
	CONTRIBUTOR	MODERATOR	APPROVER
Home & common sections e.g., FAQs, Help etc.			
Who's Who, Organization Chart, Circulars / Notifications	<Preferably Admin/ Personnel Deptt>	<Preferably Admin/ Personnel Deptt HoD>	<Preferably Web Information Manager>
<Section2: Department 1>	<Preferably Deptt-1>	<Preferably HOD>	<Preferably Web Information Manager>
<Section 3: Department 2>	<Preferably Deptt-2>		

Content Archival (CAP) policy | 5.4.3c

Purpose

Government websites generally are storehouses of a large number of documents and reports, which are of relevance and importance to specific audiences as well as citizens at large. Many times, these documents also have historical importance and are also referred extensively for academic and research purposes. These documents can be kept for online access only for a specific period of time and need to be moved to offline archives on the expiry of the pre-decided duration. This is important since these old documents sometimes need to be referred to for regulatory or legal purposes.

The Departments MUST have a clear-cut Archival Policy with regard to such old documents stating for how long would they be kept online, when would they be moved to offline archives and if/when would they be permanently deleted or purged.

Content Archival Policy

The <section names e.g., visitor statistics, newsletter and spotlight items> will be online archived automatically after entering <yth year> from the date of their publishing.

<Name of Ministry / Department / Organization> maintains online archives for a period of <x years> to allow for the retrieval of content which has expired.

<Schemes, Tenders, Forms, Recruitment Notices> which have been withdrawn, or discontinued, or have exceeded <x years> after archiving, may be expunged.

Content Review (CRP) policy | 5.4.3d

Purpose

Every piece of content appearing on the Government website should be reviewed after a pre-decided duration for its accuracy, relevance and currency. All Government Departments MUST formulate a proper web Content Review Policy (CRP) depending upon the nature of their content and if possible, also publish the policy on their website.

Content Review Policy (CRP)

The <Name of Ministry / Department / Organization Website / Portal / Web Application> is the face of the Government disseminating government information and services. This content Review Policy has been formulated to keep the content on the <Website / Portal / Web Application> current and up-to-date. Since the type of the content on the <Name of Ministry / Department / Organization Website / Portal / Web Application> varies, different Review timelines are defined for the diverse content elements.

This Review Policy is based on different types of content elements, their validity and relevance as well as the archival policy.

As a general rule

The entire website content shall be reviewed in a phased manner over a period of <x months> to ensure the currency of the content. The exception to the above is listed below

Content Review Timeline:

SECTION	REVIEW PERIODICITY
Home Page	<periodicity e.g.,Daily>
News Page	Daily
Who's who list	As and when required
Newsletter, Circulars, Notifications etc.	No review required
Acts, Rules	<periodicity e.g., 1 year>

Hyper linking Policy | 5.4.3e

Purpose:

Since Government websites receive queries and requests from owners of other websites who might want to provide a hyperlink to their web pages, every Indian Government website must have a comprehensive and clear-cut hyperlinking policy defined and spelt out for those who wish to hyperlink content from any of its sections. The hyperlinking policy enumerates the detailed criteria and guidelines with respect to hyperlinks with other sites. The basic hyperlinking practices and rules should ideally be common across the websites of any Government entity e.g., State/ Ministry.

Hyperlinking policy Links to external websites/portals

At many places in this <Website / Portal / Web Application>, you shall find links to other <Websites/ Portals/Web applications/Mobile apps>.

These links have been placed for your convenience. <Department Name> is not responsible for the contents of the linked destinations and does not necessarily endorse the views expressed in them. Mere presence of the link or its listing on this <Website / Portal / Web Application> should not be assumed as endorsement of any kind. We cannot guarantee that these links will work all the time and we have no control over availability of linked destinations.

Links to <Website / Portal / Web Application> by other websites

We do not object to you linking directly to the information that is hosted on this <Website / Portal/ Web Application> and no prior permission is required for the same. However, we would like you to inform us about any links provided to this <Website / Portal / Web Application> so that you can be informed of any changes or updates therein. Also, we do not permit our pages to be loaded into frames on your site. The pages belonging to this <Website / Portal / Web Application> must load into a newly opened browser window of the User.

Terms & Conditions | 5.4.3f

Purpose

With the increased proliferation of the Internet, more and more citizens are accessing information from Government websites. Clearly defined Terms & Conditions including well-worded disclaimers regarding the usage of websites must be present on every Indian Government website. Terms & Conditions address the following aspects:

- Ownership Details
- Legal Aspects
- Usage Policy of Content
- Responsibility towards hyperlinked Sites

Terms & Conditions:

This website is designed, developed and maintained by <Name of Department>, Government of India.

Though all efforts have been made to ensure the accuracy and currency of the content on this website, the same should not be construed as a statement of law or used for any legal purposes. In case of any ambiguity or doubts, users are advised to verify/check with the Department(s) and/or other source(s), and to obtain appropriate professional advice.

Under no circumstances will this Department be liable for any expense, loss or damage including, without limitation, indirect or consequential loss or damage, or any expense, loss or damage whatsoever arising from use, or loss of use, of data, arising out of or in connection with the use of this website.

These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the jurisdiction of the courts of India.

The information posted on this website could include hypertext links or pointers to information created and maintained by non-Government /

private organisations. <Name of Department> is providing these links and pointers solely for your information and convenience. When you select a link to an external website, you are leaving the <Name of Department> website and are subject to the privacy and security policies of the owners/sponsors of the external website.

<Name of Department> does not guarantee availability of linked pages at all times.

<Name of Department> cannot authorize use of copyrighted materials contained in the linked website. Users are advised to request such authorisation from owners of linked websites.

<Name of Department> does not guarantee that linked websites comply with Indian Government Web Guidelines.

Website Monitoring Plan | 5.4.3g

Purpose:

Hosting Service Provider should provide web server statistics required for performance evaluation on a regular basis. If possible, online access to the traffic analysis should be provided so that the Department can access the traffic analysis at any point of time for the purpose of evaluation.

Performance Evaluation & Monitoring Process

(i) Application Performance

Application performance is regularly monitored using <CMS-specific tools, or other tools> available to application administrator.

This may include CMS specific Status Report (which is a comprehensive report based on various parameters of application availability, security, performance and access restrictions) OR list any other reports available with the tools being used to monitor application performance.

(ii) Server Performance

Host of servers including webserver and database servers are monitored periodically to ensure high availability and smooth functioning of the <Name of Ministry / Department / Organization Website / Portal / Web Application>.

(iii) Download Speeds

- Frequency: <frequency e.g., daily / weekly etc.>
- Process: Using the open-source tools and add-ons available with browsers <like Firebug's netstat for Mozilla> the download speed of pages across the portal are checked on different Internet connectivity.
- Pages are tested at various connections and slow loading pages are identified and corrected (once).

(iv) Availability of Portal

Availability of <Name of Ministry / Department / Organization Website /

Portal / Web Application> is monitored at intervals of <frequency> by the <Website Monitoring team (if there is a dedicated monitoring team)>. Homepage and important landing pages have been marked and provided to monitoring team for regular check.

Privacy Policy | 5.4.3h

Purpose

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Privacy Policy

<Name of Website / Portal / Web Application (e.g., India Portal, DoT website, TRAI website, IRCTC etc.)> does not automatically capture any specific personal information from you (like name, phone number or e-mail address), that allows us to identify you individually. If you choose to provide us with your personal information, like names or addresses, when you visit our website, we use it only to fulfil your request for information. To use the <xyz section(s)>, this website <**requires user registration/does not require registration**. <[If user registration is required] **Information so collected is used to facilitate interaction**>.

We do not sell or share any personally identifiable information volunteered on this site to any third party (public/private). Any information provided to this website will be protected from loss, misuse, unauthorized access or disclosure, alteration, or destruction.

We gather certain information about the User, such as Internet protocol (IP) address, domain name, browser type, operating system, the date and time of the visit and the pages visited. We make no attempt to link these addresses with the identity of individuals visiting our site unless an attempt to damage the site has been detected.

Use of Cookies:

A cookie is a piece of software code that an internet web site sends to your browser when you access information at that site. A cookie is stored as a simple text file on your computer or mobile device by a website's server and only that server will be able to retrieve or read the contents of that cookie. Cookies let you navigate between pages efficiently as they store your preferences, and generally improve your experience of a website.

<We are using following types of cookies in our site:

- Analytics cookies for anonymously remembering your computer or mobile device when you visit our website to keep track of browsing patterns.
- Service cookies for helping us to make our website work efficiently, remembering your registration and login details, settings preferences, and keeping track of the pages you view.
- Non-persistent cookies a.k.a per-session cookies. Per-session cookies serve technical purposes, like providing seamless navigation through this website. These cookies do not collect personal information on users and they are deleted as soon as you leave our website. The cookies do not permanently record data and they are not stored on your computer's hard drive. The cookies are stored in memory and are only available during an active browser session. Again, once you close your browser, the cookie disappears.>

<You may note additionally that when you visit sections of <Website / Portal / Application> where you are prompted to log in, or which are customizable, you may be required to accept cookies. If you choose to have your browser refuse cookies, it is possible that some sections of our web site may not function properly.>

Contingency Management Plan | 5.4.3i

Purpose

The website 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 of the Government websites to deliver information and services on a 24x7 basis. Hence, all efforts should be made to minimise the downtime of the website as far as possible.

It is therefore necessary that a proper Contingency Plan MUST be prepared in advance to handle any eventualities and restore the site in the shortest possible time.

Contingency Management Plan & Disaster Recovery Process

<Name of Ministry / Department / Organization Website / Portal / Web Application> has been placed in protected zones with implementation of firewalls and IDS (Intrusion Detection System) and high availability solutions.

(i) Defacement Protection

- <Name of Ministry / Department / Organization Website / Portal / Web Application> is audited for protection against Security & Performance degradation.
- Any application level modification on the <Name of Ministry / Department / OrganizationWebsite / Portal / Web Application> requires re-audit.
- All the server configuration and logs are monitored timely.
- Only System administrator users are allowed to access the servers for doing administration and configuration tasks.
- All the backend servers are under lock and net secured.
- Contents are updated through a <secure FTP using VPN / CMS>.

(ii) Monitoring

There are <two> ways of monitoring the defacement of <Name of Ministry / Department / Organization Website / Portal / Web Application>.

- Cyber security division monitors by analyzing the log files.
- <Website Monitoring Team specifics> also monitors the <Name of Ministry / Department / Organization Website / Portal / Web Application> after

interval of every <frequency> for possible defacement or undesirable change in the <Name of Ministry / Department / Organization Website / Portal / Web Application>. (in case the site has a dedicated monitoring team).

(iii) Defacement Response Plan

In case of any eventuality, whoever notices the defacement (either Website Monitoring Team or Cyber Security) informs the Web Information Manager on phone as well as through mail. NIC Cyber Security Division or Help Desk also informs the Administrator. <Name of Ministry / Department / Organization Website / Portal / Web Application> on telephone and also by mail.

S.NO.	PERSON IN CHARGE	DESIGNATION	MAIL ADDRESS	TELEPHONE NUMBER
1.	<Name>			
2.	<Name>			
3.	<Name>			

As soon as the <Name of Ministry / Department / Organization Website / Portal / Web Application> Server Administrator gets the information regarding the defacement, s/he takes the following steps.

- According to the degree of defacement, the site is stopped or continued partially.
- Log files are analyzed to troubleshoot the source of defacement and blocking of the service.
- Type of the defacement is analyzed and fixed.
- The Portal Service is started from the DR site in case of complete loss of data or during long downtime.
- Log files are given to the security division for analysis.
- Based on security recommendations, all vulnerabilities are fixed and the application is re-audited.
- The affected/corrupted content and the site are restored from the backup.

Time for Restoration after defacement

The time taken for restoration depends on the degree of defacement and services affected by the defacement. Ideally it will take <x hours> for the restoration.

(iv) Natural Calamity Response Plan

There could be circumstances whereby due to some natural calamity (it may be due to any reason that is beyond control of any person), the entire data centre where the <Name of Ministry / Department / Organization Website / Portal / Web Application> has been hosted gets destroyed or ceases to exist. In such case first of all the In-charge of National Data Centre will declare the natural calamity and would instruct the sites to be started from the DR site, which is located at <Name of Data Center Location>.

Security Policy | 5.4.3j

Purpose

Security is of paramount concern to owners as well as consumers of the website. A lot of security threats are handled at data centres and server administrator level where the website/application is hosted. Website/ Application developers should however be sensitive about security aspects, as a lot of security threats arise due to vulnerability of application software code.

These application driven attacks sometimes turn out to be quite fatal. Best Practices to follow while developing web applications using various technologies are available on CERT-IN website (http:// www.cert-in.org.in) as well as in internet space. Developers should read, understand and follow these Best Practices during development. NIC as well as CERT. IN have empaneled a number of agencies to conduct the security audit of applications.

Security policy

- <Name of Ministry / Department / Organization Website / Portal / Web Application> has been placed in protected zones with implementation of firewalls and IDS (Intrusion Detection System) and high availability solutions.

- Before launch of the <Name of Ministry / Department / Organization Website / Portal / Web Application>, simulated penetration tests have been conducted. Penetration testing has also been conducted <x times> after the launch of the <Name of Ministry / Department / Organization Website / Portal / Web Application>.
- <Name of Ministry / Department / Organization Website / Portal / Web Application> has been audited for known application-level vulnerabilities before the launch and all the known vulnerabilities have been addressed.
- Hardening of servers has been done as per the guideline of Cyber Security division before the launch of the <Name of Ministry / Department / Organization Website / Portal / Web Application>.
- Access to web servers hosting the <Name of Ministry / Department / Organization Website / Portal / Web Application> is restricted both physically and through the network as far as p ossible.
- Logs at <x number> different locations are maintained for authorized physical access of <Name of Ministry / Department / Organization Website / Portal / Web Application> servers.
- Web-servers hosting the <Name of Ministry / Department / Organization Website / Portal / Web Application> are configured behind IDS, IPS (Intrusion Prevention System) and with system firewalls on them.
- All the development work is done on a separate development environment and is well tested on the staging server before updating it on the production server.
- After testing properly on the staging server, the applications are uploaded to the production server using SSH and VPN through a single point.
- The content contributed by/from remote locations is duly authenticated & is not published on the production server directly. Any content contributed has to go through the moderation process before final publishing to the production server.
- All contents of the web pages are checked for intentional or

unintentional malicious content before final upload to web server pages.

- Audit and Log of all activities involving the operating system, access to the system, and access to applications are maintained and archived. All rejected accesses and services are logged and listed in exception reports for further scrutiny.
- Help Desk staff at the <Identify Monitoring Team> monitor the <Name of Ministry / Department / Organization Website / Portal / Web Application> at intervals of <frequency> to check the web pages to confirm that the web pages are up and running, that no unauthorized changes have been made, and that no unauthorized links have been established.
- All newly released system software patches; bug fixes and upgrades are expediently and regularly reviewed and installed on the web server.
- On Production web servers, Internet browsing, mail and any other desktop applications are disabled. Only server administration related tasks are performed.
- Server passwords are changed at the interval of <x number> months and are shared by <y number> persons <a name> and <b name>.
- <a name> and <b name> have been designated as Administrator for the <Name of Ministry / Department / Organization Website / Portal / Web Application> and shall be responsible for implementing this policy for each of the web servers. The administrator shall also coordinate with the Audit Team for required auditing of the server(s).
- <Name of Ministry / Department / Organization Website / Portal / Web Application> has been re-audited for the application-level vulnerability after major modification in application development [Not applicable at first launch].

Compliance Audit

The <Name of Ministry / Department / Organization Website / Portal / Web Application> has been audited before launch and has complied with all the points mentioned in the policies document of the Cyber Security Group mentioned above.

<Name of Ministry / Department / Organization Website / Portal / Web Application> has also been subjected to an automated risk assessment performed through vulnerability identification software before and after the launch and all the known vulnerabilities have been addressed.

Validation & Testing Process | 5.4.3k

Purpose of the process

The code of the webpages, scripts and applications may be tested manually or with automated tools to ensure that the quality of web content is maintained and all compliance related guidelines or adhered to.

Validation & Testing Process

<Name of Ministry / Department / Organization Website / Portal / Web Application> is tested regularly <manually and through automated testing> tools by the Technical Manager for the following parameters.

(A) Quality Testing

(i) Broken Links

- Frequency: <Daily/Weekly etc.>
- Process: <Name of Ministry / Department / Organization Website / Portal / Web Application> is monitored for broken links <manually / automated tool>.
- Action taken: The reviewer sends a list of broken links to the quality manager who rectifies them personally.

(ii) Spelling Errors

- Frequency: <Daily / Weekly etc.>
- Process: By the QM <manually / through automated tool>. It is the responsibility of the Quality Manager to get the spelling mistakes rectified from the concerned person depending on whether the mistake is in the static or dynamic portion of content.

- Action taken: The Quality Manager sends a mail to the concerned person who rectifies the mistake and responds back to the Quality Manager.

(iii) Metadata

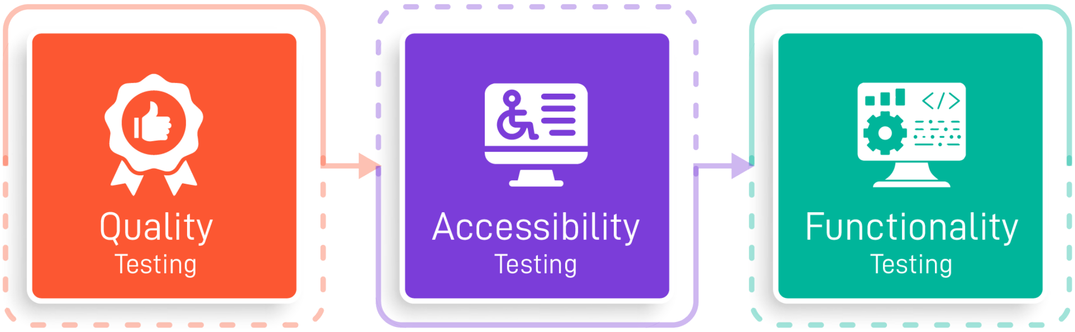
- Frequency: <Weekly / Monthly etc.>
- Process: Based on the web analyzer tool reports the pages are checked for proper meta tags by the Quality Manager.
- Action taken: The Quality Manager modifies the metadata if required.

(B) Accessibility Testing

Conformance with respect to W3C norms, Tools such as <list available tools> are used for testing.

(C) Functionality Testing

- Frequency: <Weekly / Monthly etc.>
- Process: Interactive components like forms etc. are tested for functionality issues.
- Action taken: The Quality Manager informs the concerned person through mail in case of any problem and receives a confirmation mail on rectification of the same.



6. APPENDIX

6.1. GIGW Compliance Matrix

GIGW Compliance Matrix | 6.1

S.No.	Quality Guidelines	Risks Addressed
1	Association to Government is demonstrated using Emblem/Logo in proper ratio and colour, prominently displayed on the homepage/homescreen of the website/app.	Q8
2	Ownership information is displayed on thehomepage/ homescreen and on all important entry pages/screens of the website/app and each subsequent page/screen is a standalone entity in terms of ownership, navigation and context of content.	Q8
3	Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned.	Q3
4	Due permissions have been obtained for publishing any content protected by copyright.	Q3
5	Homepage/homescreen of website displays the last updated/reviewed date.	Q7
6	Complete information including title, size, format and usage instructions is provided for all downloadable material.	Q7
7	Statement: With respect to each, Circular, Notification, Document, Form, Scheme, Service and Recruitment notice, the following should be clearly listed on the Website: (a) Complete title (b) Language (if other than English) (c) Purpose/procedure to apply (as applicable) (d) Validity (if applicable)	Q7
8	All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are removed from the website and/or placed into the archives as per the archival policy.	Q7

S.No.	Quality Guidelines	Risks Addressed
9	All information about the government organisation, useful for the citizen and other stakeholders, is present in the 'About Us' section and a mechanism is in place to keep the information up to date.	Q6, Q7
10	Website has a 'Contact Us' page providing complete contact details of important functionaries in the government organisation and this is linked from the homepage/homescreen and all relevant places on the website/app.	Q6, Q7
11	Feedback is collected through online forms and a mechanism is in place to ensure timely response to feedback/queries received through the website.	Q10
12	Website provides a prominent link to the 'National Portal' from the homepage and subsequent pages belonging to the National Portal load in the new browser window.	Q7
13	The website has been tested on multiple browsers. Hindi/ Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout).	Q9
14	The website has a readily available Help section linked from all pages of the website.	Q6,Q7
14	Website uses Cascading Style Sheets (CSS) to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes.	Q9
16	Website is readable even when style sheets are switched off or not loaded.	Q9
17	Proper page title and language attribute along with metadata for page like keywords and description are appropriately included.	Q9
18	Minimum content as prescribed in the guidelines is present on the homepage/homescreen and all subsequent pages/screens.	Q6, Q7
19	Data tables have been provided with necessary tags/ markup.	Q9

S.No.	Quality Guidelines	Risks Addressed
20	Content of the web page prints correctly on an A4 size paper	Q9
21	API integration with key government platforms (India Portal, DigiLocker, Aadhaar, Single-Sign-On, MyGov, Data Platform, MyScheme) and similar websites of the government organisation must be enabled for seamless exchange of Information and data.	Q7, Q8, Q10
22	The government organisation must ensure a consistent user experience and visual identities across all its websites/apps.	Q1, Q4, Q9
23	Websites/apps must provide integration with popular social media.	Q1, Q3, Q5, Q7
24	Website is in the nic.in or gov.in domain. Educational Institutions and Research and Academic Institutions, which are eligible for registration under 'gov.in' may use 'edu.in', 'res.in' or 'ac.in' domains.	Q8
25	The language is free from spelling and grammatical errors.	Q7, Q9

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
1	All non-text content that is presented to the user has a text alternative that serves theequivalent purpose, except for the situations listed below.	WCAG 2.1-1.1.1	A1
2	For pre-recorded audio-only and pre-recorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labelled as such: (a) Pre-recorded Audio-only: An alternative for time-based media is provided that presents equivalent information for pre-recorded audio-only content. (b) Pre-recorded Video-only: Either an alternative for time-based media or an audio track is provided that presents equivalent information for pre-recorded video-only content.	WCAG 2.1-1.2.1	A1
3	Captions are provided for all pre-recorded audio content in synchronized media, exceptwhen the media is a media alternative for text and is clearly labelled as such.	WCAG 2.1-1.2.2	A1
4	An alternative for time-based media or audio description of the pre-recorded video content is provided for synchronized media, except when the media is a media alternative for text and is clearly labelled as such.	WCAG 2.1-1.2.3	A1
5	Captions are provided for all live audio content in synchronized media.	WCAG 2.1-1.2.4	A1

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
6	Audio description is provided for all pre-recorded video content in synchronized	WCAG 2.1-1.2.5	A1
7	Information, structure and relationships conveyed through presentation can be programmatically determined or are available in text.	WCAG 2.1-1.3.1	A6, A9
8	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	WCAG 2.1-1.3.2	A6, A9
9	Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, colour, size, visual location, orientation, or sound.	WCAG 2.1-1.3.3	A1, A2, A3, A4
10	Content does not restrict its view operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.	WCAG 2.1-1.3.4	A4, A5
11	The purpose of each input field collecting information about the user can be programmatically determined when: (a) The input field serves a purposeidentified in the Input Purposes for User Interface Components section; and (b) The content is implemented using technologies with support for identifying the expected meaning for form input data.	WCAG 2.1-1.3.5	A6

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
12	Colour is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	WCAG 2.1-1.4/1	A1
13	If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume ndependently from the overall system volume level.	WCAG 2.1-1.4.2	A4, A5
14	The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: Large Text: (18 pt. or 14 pt. bold) Large-scale text and images of large-scale text have a contrast ratio of at least 3:1. Incidental: Text or images of text that are part of an inactive user interface components, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. Logotypes: Text that is part of a logo or brand name has no contrast requirement.	WCAG 2.1-1.4.3	A4, A5
15	Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality.	WCAG 2.1-1.4.4	A1, A4
16	If the technologies being used can achieve the htt visual presentation, text is used to convey information rather than	WCAG 2.1-1.4.5	A1

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
	images of text except for the following: Customizable: The image of text can be visually customised to the user's requirements. Essential: A particular presentation of text is essential to the information being conveyed		
17	Content can be presented without loss of information or functionality and without requiring scrolling in two dimensions for: Vertical scrolling content at a width equivalent to 320 CSS pixels. Horizontal scrolling content at a height equivalent to 256 CSS pixels. Except for parts of the content which require a two-dimensional layout for usage or meaning.	WCAG 2.1-1.4.10	A6
18	The visual presentation of the following has a contrast ratio of at least 3:1 against adjacent colour(s): (a) User Interface Components: To information required to identify user interface components and states, except for inactive components or where the appearance of the component is determined by the user agent and not modified by the author. (b) Graphical Objects: Parts of graphics required to understand the content, except when a particular presentation of graphics is essential to the information being conveyed.	WCAG 2.1-1.4.11	A6

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
19	In content implemented using markup languages that support the following text style properties, no loss of content or functionality occurs by setting all of the following and by changing no other style property: Line height (line spacing) to at least 1.5 times the font size. (a) Spacing following paragraphs to at least 2 times the font size. (b) Letter spacing (tracking) to at least 0.12 times the font size. (c) Word spacing to at least 0.16 times the font size. (d)Exception: Human languages and scripts that do not make use of one or more of these text style properties in written text can conform using only the properties that exist for that combination of language and script.	WCAG 2.1-1.4.12	A6
20	Where receiving and then removing pointer hover or keyboard focus triggers additional content to become visible and then hidden, the following are true: Dismissible: A mechanism is available to dismiss the additional content without moving pointer hover or keyboard focus unless the additional content communicates an input error or does not obscure or replace other content.	WCAG 2.1-1.4.12	A4, A5, A6

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
	Hover-able: If pointer hover can trigger the additional content, then the pointer can bemoved over the additional content without the additional content disappearing. Persistent: The additional content remains visible until the hover or focus trigger is removed, the user dismisses it, or its information is no longer valid.		
21	All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints.	WCAG 2.1-2.1.1	A5
22	If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away.	WCAG 2.1- 2.1.2	A5
23	If a keyboard shortcut is implemented in content using only letter (including upper-and lower-case letters), punctuation, number, or symbol characters, then at least one of the following is true: Turn off: A mechanism is available to turn the shortcut off. Remap: A mechanism is available to	WCAG 2.1-2.1.4	A5

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
	remap the shortcut to include one or more non-printable keyboard keys (e.g., Ctrl, Alt). Active only on focus: The keyboard shortcut for a user interface component is only active when that component has focus		
24	For each time limit that is set by the content, at least one of the following is true: Turn off: The user is allowed to turn off the time limit before encountering it; or Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or (a) Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the spacebar") and the user is allowed to extend the time limit at least ten times; or (b) Real-time Exception: The time limit is a required part of a real-time event (for example, an auction) and no alternative to the time limit is possible; or (c) Essential Exception: The time limit is essential and extending it would invalidate the activity; or (d) 20 Hour Exception: The time limit is longer than 20 hours.	WCAG 2.1-2.2.1	A4

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
25	For moving, blinking, scrolling, or auto-updating information, all of the following are true: Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential.	WCAG 2.1-2.2.2	A2, A4
26	Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds.	WCAG 2.1-2.3.1	A2
27	A mechanism is available to bypass blocks of content that are repeated on multiple Web pages.	WCAG 2.1-2.4.1	A6
28	Web pages have titles that describe the topic or purpose.	WCAG 2.1-2.4.2	A6
29	If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in	WCAG 2.1-2.4.3	A6

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
	an order that preserves meaning and operability.		
30	The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general.	WCAG 2.1-2.4.4	A6
31	More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a	WCAG 2.1-2.4.5	A6
32	Headings and labels describe topic	WCAG 2.1-2.4.6	A6, A
33	Any keyboard operable user interface has a mode of operation where the keyboard focus indicator is visible.	WCAG 2.1-2.4.7	A4
34	All functionality that uses multipoint or path-based gestures for operation can be operated with a single pointer without a path-based gesture, unless a multipoint or path-based gesture is essential.	WCAG 2.1-2.5.1	A4
35	For functionality that can be operated using a single pointer, at least one of the following is true: No Down-Event: The down-event of the pointer is not used to execute any part of the function. Abort or Undo: Completion of the function is on the up-event and a mechanism is available to abort the function before completion or to undo the function after completion.	WCAG 2.1-2.5.2	A4

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
	Up Reversal: The up-event reverses any outcome of the preceding down-event. Essential: Completing the function on the down-event is essential.		
36	For user interface components with labels that include text or images of text, the name contains the text that is presented visually.	WCAG 2.1-2.5.3	A9
37	Functionality that can be operated by device motion or user motion can also be operated by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: Supported Interface: The motion is used to operate functionality through an accessibility supported interface. Essential: The motion is essential for the function and doing so would invalidate the activity. Functionality that can be operated by device motion or user motion must also be operable by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: Supported Interface: The motion is used to operate functionality through an accessibility supported interface. Essential: The motion is essential for the	WCAG 2.1-2.5.4	A5

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
	function and doing so would invalidate the activity.		
38	The default human language of each Web page can be programmatically determined.	WCAG 2.1-3.1.1	A1, A A7
39	The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language and words or phrases that have become part of the vernacular of the immediately surrounding text.	WCAG 2.1-3.1.2	A1, AA7
40	When any user interface component receives focus, it does not initiate a change of context.	WCAG 2.1-3.2.1	A6
41	Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behaviour before using the component.	WCAG 2.1-3.2.2	A6
42	Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user.	WCAG 2.1-3.2.3	A6
43	Components that have the same functionality within a set of Web pages are identified consistently.	WCAG 2.1-3.2.4	A6
44	If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.	WCAG 2.1-3.3.1	A6
45	Labels or instructions are provided when content requires user input.	WCAG 2.1-3.3.2	A9

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
46	If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardise the security or purpose of the content.	WCAG 2.1-3.3.3	A4, A
47	For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: (a) Reversible: Submissions are reversible. (b) Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. (c) Confirmed: A mechanism is available for reviewing, confirming and correcting information before finalising the submission.	WCAG 2.1-3.3.4	A8
48	In content implemented using markup languages, elements have complete start and tags, elements are nested according to their specifications, elements do not contain duplicate attributes and any IDs are unique, except where the specifications allow these features.	WCAG 2.1-4.1.1	A6

S.No.	Accessibility Guidelines	Reference	Risks Ad-dressed
49	For all user interface components (including but not limited to form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.	WCAG 2.1-4.1.2	A6
50	In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus.	WCAG 2.1-4.1.3	A6

S.No.	Security Guidelines	Risks Addressed
1	Ensure that the website, web application, web portal or mobile app is Security Audited and an Audit Clearance certificate is issued by NIC, STQC or a CERT-In empanelled vendor before hosting in production environment.	S1- S15
2	Hosting Environment must be secured for ensuring confidentiality, integrity and availability (CIA).	S1- S15
3	Website has the Security Policy, Privacy Policy and the Contingency Management Plan clearly defined policies and plans approved by the government organisation.	S1- S15

S.No.	Lifecycle Management Guidelines	Risks Addressed
1	The government organization has nominated a WIM as defined in the guidelines.	Q1
2	It has been ensured that all stationery of the government organization as well as advertisements/ public messages issued by the government organization concerned prominently display the URL of the web site.	Q2
3	Website has the following clearly defined policies and plans approved by the WIM. (a) Copyright Policy (b) Content Contribution, Moderation and Approval (CMAP) policy (c) Content Archival (CAP) policy (d) Content Review (CRP) policy (e) Hyper linking Policy (f) Privacy Policy (g) Terms & Conditions (h) Website Monitoring Plan. (i) Contingency Management Plan (j) Security Policy	Q3, Q4, Q5, Q7
4	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.	Q4
5	It is ensured through content moderation and approval policy that Website content is free from offensive/ discriminatory language.	Q7
6	Documents/Pages in multiple languages are updated simultaneously.	Q7

S.No.	Lifecycle Management Guidelines	Risks Addressed
7	Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors.	Q7
8	There are no links to 'under construction' pages.	Q7
9	Documents are provided either in HTML or other accessible formats.	Q9
10	Website is bilingual with a prominent language selection link and uses Unicode characters.	Q9, Q6, Q7

7. CONTENT MANAGEMENT SYSTEM

Content Management System | 5.7

A Content Management System (CMS) is a robust system that enables efficient content management and display on a user interface. To meet today's standards, a CMS should encompass the following essential requirements:

1. Content Creation:

Content creation functionality is crucial for authors (content contributors) utilizing the CMS. An effective authoring process enables users to easily adopt the CMS. The CMS should provide the following features for effective content contribution:

(a) Single-sourcing (content reuse):

The CMS should allow content to be contributed once and reused in different contexts. For example, a circular/notification/picture/press release/new scheme/forms should be up dated on the website and made available under various sections such as Downloads, What's New, and Press Releases, without the need to upload it multiple times.

(b) Metadata creation:

Metadata, such as creator, subject, and keywords, should be captured by the CMS. Including keywords for pictures or scanned images makes the information searchable.

(c) User-friendly inter face and efficiency:

The CMS should enable authors to create pages without requiring HTML or technical knowledge. An effective CMS should be easy to use and maintain.

2. Content Management:

To effectively manage content, a CMS should include the following functionality and features:

(a) Version control and archiving:

The CMS should have login-based access to track details such as content creators, modifications, and approvals. These features ensure accountability for content creators and approvers. Additionally, the CMS should automatically archive content after reaching a predefined age, maintaining archives of old and relevant content while displaying only current content.

(b) Workflow:

A CMS should enable decentralized content management, allowing content input at the source. For example, the Personnel department would be responsible for updating content related to changes in responsibility, designation, and physical location. The CMS should support customizable workflows, accommodating changes in the organizational structure. Multiple levels of personnel should contribute, review, and approve content to ensure accuracy.

(c) Reporting:

The CMS should provide a wide range of reports for users and administrators. It should proactively send alerts for content that needs review, update, archival, or permanent purging. This feature helps maintain the currency of content. Additionally, the CMS should generate reports on usage statistics, such as the most popular pages, daily usage, search engine usage, and downloads. Customized reporting support is also desirable.

3. Content Publishing:

A CMS should provide the following publishing functionality and features:

(a) Stylesheets and support for multiple formats:

Stylesheets control the final appearance of content, separating it from its presentation. This separation allows the CMS to publish content in multiple formats, such as HTML (web), printed, PDF, handheld (WAP), and any emerging formats. Separating content from presentation during authoring ensures high-quality output in every format.

(b) Page templates:

Page templates define the overall layout of pages. Ideally, a non-technical interface should be provided for managing page layout. Using templates helps maintain consistency, as the page layout doesn't need modification whenever content in specific sections is updated.

4. Content Presentation:

To ensure valuable content for users, a CMS must meet certain standards, including:

(a) Usability:

The CMS should focus on aspects such as ease of use, learnability, and efficiency. Conducting tests with real users on prototype designs can assure usability.

(b) Accessibility:

The CMS must publish content that adheres to standards like the W3C Web Content Accessibility Guidelines (WCAG). Conforming to accessibility standards ensures content remains accessible to all users, regardless of ability or device, and remains functional across various browsers.

(c) Valid markup:

All pages must conform to the current HTML specification. This ensures maximum compatibility across different browsers and platforms.

By incorporating these features and adhering to contemporary standards, a CMS can effectively meet the requirements of content creation, management, publishing, and presentation. These enhancements ensure that the CMS remains relevant and up to date in today's rapidly evolving digital landscape.

By implementing a modern CMS, organizations can achieve the following benefits:

1. Streamlined Content Creation:

The CMS provides an intuitive and user-friendly interface, allowing authors to create and contribute content without the need for technical expertise. This streamlines the content creation process and empowers content contributors to focus on generating high-quality content.

2. Efficient Content Management :

With version control and archiving features, the CMS ensures accountability by tracking content creation, modifications, and approvals. It also automatically archives outdated content, maintaining a clean and up-to-date content repository. The customizable workflow facilitates collaboration among various stakeholders, ensuring accurate and timely content updates.

3. Comprehensive Reporting:

The CMS offers a wide range of reports for users and administrators, providing valuable insights into content performance and usage. Proactive alerts help users keep track of content that requires attention, while usage statistics enable data-driven decision-making and optimization of popular areas.

4. Flexible Publishing Options:

With support for multiple formats and stylesheets, the CMS enables content to be published in various output formats such as web, print, PDF, and mobile devices. The separation of content from presentation allows for consistent branding and layout across different channels while catering to diverse user preferences.

5. Enhanced User Experience:

Usability testing and adherence to accessibility standards ensure that the CMS delivers an exceptional user experience. Users can easily navigate and interact with the content, regardless of their abilities or the devices they use. Valid markup ensures cross-browser compatibility and optimal performance.

Popular Open-Source CMS Examples: Several open-source CMS platforms are widely used and trusted. Here are some examples:

1. WordPress:

One of the most popular CMS platforms globally, WordPress offers a user-friendly interface, a vast selection of plugins and themes, and a large community for support.

2. Joomla:

Joomla is known for its flexibility and scalability, making it suitable for small websites and large enterprises alike. It offers a robust set of features and a user-friendly admin interface.

3. Drupal:

Drupal is a highly customizable CMS platform that caters to complex and large-scale websites. It provides extensive functionality, strong security features, and a dedicated developer community.

By considering the essential requirements outlined above and selecting a modern CMS, organizations can streamline content creation, efficiently manage content, generate comprehensive reports, publish content in various formats, and deliver an enhanced user experience. Open-source CMS platforms like WordPress, Joomla, and Drupal are popular choices that offer the necessary features and community support. Implementing a suitable CMS empowers organizations to effectively manage their content lifecycle, improve productivity, maintain brand consistency, and deliver engaging experiences to their users. The adaptability and scalability of a modern CMS also enable organizations to meet future content management needs as technology continues to evolve.

GIGW

GUIDELINES FOR INDIAN GOVERNMENT WEBSITES

COMPLIANCE & CERTIFICATION HANDBOOK

Data Centre and Web Services Group

National Informatics Centre

A-Block, CGO Complex, Lodhi Road, New Delhi - 110003

Email : webguidelines@nic.in