

Note : Pls remove all red ink text after preparation of final document  
from this exercise book.

Draft for preparation your own manual

**Document number:**

Issue number :

Date of Issue :

Revision number:

Date of Revision :

## Exercise Book

# Website Quality Manual

(for Public Website)

URL: .....

*Complete address*

ō ō ō ō ō ō ō ō ō ō ō ō ō ō ..

ō ō

ō .

*Month, Year*

**Document Revision History**

<b>Issue No.</b>	<b>Rev. No.</b>	<b>Dated</b>	<b>Issued By</b>	<b>Authorized By</b>	<b>Remarks</b>

## Content

### **A. Background information:**

1. Scope of the website quality manual
2. About the Ministry/Department/Organisation/Cells
3. Website address ,Data Centre & Hosting organisation
4. Purpose of the website
5. Objectives of the website
6. Responsibility & Authority
7. List of Platform (H/W, S/W) & Web Technologies used
8. Use of Contractors/ Subcontractors

### **B. Policies (relevant DARPG guidelines clause):**

1. Copyright policy (clause 3.1.1)
2. Hyper Linking policy (clause 3.2.1)
3. Privacy policy (clause 3.4.2)
4. Content Contribution, Moderation & Approval policy (CMAP) (clause 5.2.1)
5. Web Content Review policy (CRP) (clause 5.2.3)
6. Content Archival policy (clause 10.4)
7. Security policy (clause 7.7.2)
8. Website Monitoring policy (clause 10.3)

### **C. Responsibility and Authority (website management team):**

- Web Information Manager (clause 10.1.1)
- Technical Manager (optional)

### **D. Plans:**

1. Contingency plan in the event of defacement / natural calamity (clause 8.3)
2. Website monitoring plan (clause 10.3)

### **E. Organisation Structure**

1. Website developer
2. IT service provider
3. Content management
4. Data center / Hosting organisation
5. User
6. Application Developer

### **G. Compliance Statement**

1. Guidelines for Indian Government Websites (refer annexure I attached)
2. Legal compliance
3. Security Audit report (clause 7.7.1)

### **H. Miscellaneous:**

1. Person responsible for updating of website quality manual
2. Declaration by Website Manager

Annexure I : Compliance matrix for GIGW 2018 guidelines

## **A . Background information:**

### ***1. Scope of the website quality manual***

This Website Quality manual is the compilation of policies, processes and procedures being followed in the company for developing & maintaining a well engineered website for our clients. It aims to address site wide issues and improve the productivity of managed web operations in terms of .

- a) Locating relevant information
- b) Facilitating ease of use
- c) Reducing legal liabilities
- d) Providing for efficient development and maintenance considerations

## **2. *About the Ministry/Department/ Organization/ Cells***

**3. Website Address, Data Centre & Hosting organization**

**4. Purpose of the website**

**5. Objectives of the website**

**6. Responsibility & Authority**

<b>Activity</b>	<b>Conducted at (Division)</b>	<b>Conducted by (Responsibility)</b>
Design		
Development		
Contents		
Testing		
Monitoring		
Hosting		
Promotion		
Website Management		
Security		



## 7. List of Platform (H/W, S/W) & Web Technologies used :

The company uses the following range of technologies to offer solutions to our clients .

Example:

<b>Sl. no.</b>	<b>Technologies / Platforms used</b>	<b>Remarks</b>
1	Open source	
2	IBM Websphere	
3	Microsoft IIS/Apache	
4	SAP Netweaver	
5	Oracle	
6	BEA weblogic	

## 8. Use of Contractors / Sub Contractors

The following processes are sub-contracted -

- a) Testing (Development and Operational) (G.6)
- b) Accessibility (G.9)
- c) Maintenance (G.10)
- d) Robot exclusion elements (G.13)
- e) Content Management System

These sub-contractors are chosen as per laid down procedures (Procedure No. 000..00..)

A list of sub-contractors along with capabilities is maintained at (Deptt. name)

Their performance is monitored periodically as per procedure no. 00000 .

**B. Policies (relevant clause of Guidelines to Indian Govt. websites) :**

**Sample**

**1. Copyright policy (clause 3.1.1)**

Material featured on this site may be reproduced free of charge in any format or media without requiring specific permission. This is subject to the material being reproduced accurately and not being used in a derogatory manner or in a misleading context. Where the material is being published or issued to others, the source must be prominently acknowledged. However, the permission to reproduce this material does not extend to any material on this site, which is identified as being the copyright of a third party. Authorization to reproduce such material must be obtained from the copyright holders concerned.+

or

Material on this site is subject to copyright protection unless otherwise indicated. The material may be downloaded to file or printer without requiring specific prior permission. Any other proposed use of the material is subject to the approval of (*name of department*). Application for obtaining permission should be made to (email address of the concerned department)+

*(Write topic wise details about your organisation and website)*

## **2. Hyper Linking policy (clause 3.2.1)**

### **Sample**

We do not object to you linking directly to the information that is hosted on our site and no prior permission is required for the same. However, we would like you to inform us about any links provided to our site so that you can be informed of any changes or updation therein. Also, we do not permit our pages to be loaded into frames on your site. Our Department's pages MUST load into a newly opened browser window of the user.

or

Prior permission is required before hyperlinks are directed from any website to this site. Permission for the same, stating the nature of the content on the pages from where the link has to be given and the exact language of the Hyperlink should be obtained by sending a request at (Email address of the Department).

or

This link shall take you to a page outside the (\_\_\_\_\_) website. For any query regarding the contents of the linked page, please contact the webmaster of the concerned website.

(Write topic wise details about your organisation and website)

### 3. Privacy policy (clause 3.4.2)

#### Sample

Thanks for visiting website of \_\_\_\_\_ Department and reviewing our privacy policy.

We collect NO personal information, like names or addresses, when you visit our website. If you choose to provide that information to us, it's only used to fulfill your request for information.

We do collect some technical information when you visit to make your visit seamless. The section below explains how we handle and collect technical information when you visit our website.

#### Information collected and stored automatically

When you browse, read pages, or download information on this website, we automatically gather and store certain technical information about your visit. This information never identifies who you are. The information we collect and store about your visit is listed below:

- ~ The Internet domain of your service provider (e.g. mtnl.net.in) and IP address (an IP address is a number that is automatically assigned to your computer whenever you're surfing the web) from which you access our website.
- ~ The type of browser (such as Firefox, Netscape, or Internet Explorer) and operating system (Windows, Unix) used to access our site
- ~ The date and time you accessed our site
- ~ The pages/URLs you have visited and
- ~ If you reached this website from another website, the address of that referring website

This information is only used to help us make the site more useful for you. With this data, we learn about the number of visitors to our site and the types of technology our visitors use. We never track or record information about individuals and their visits.

#### Cookies

When you visit some websites, they may download small pieces of software on your computer/browsing device known as cookies. Some cookies collect personal information to recognize your computer in the future. We only use non-persistent cookies or ~~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.

#### If you send us personal information

We do not collect personal information for any purpose other than to respond to you (for example, to respond to your questions or provide subscriptions you have chosen). If you choose to provide us with personal information - like filling out a Contact Us form, with an e-mail address and pin code, and submitting it to us through the website - we use that information to respond to your message, and to help get you the information you've requested. We only share the information you give us with another government agency if your question relates to that agency, or as otherwise required by law.

Our website never collects information or creates individual profiles for commercial marketing. While you MUST provide an e-mail address for a localized response to

any incoming questions or comments to us, we recommend that you do NOT include any other personal information.

*(Write topic wise details about your organisation and website)*



### **Site Security**

“ For site security purposes and to ensure that this service remains available to all users, this government computer system employs commercial software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular deletion.

“ Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Indian IT Act (2000).

### **Another Example of a Privacy Policy Statement in case a website does not collect any personal data**

As a general rule, this website does not collect Personal Information about you when you visit the site. You can generally visit the site without revealing Personal Information, unless you choose to provide such information. The information received depends upon what you do when visiting the site.

#### **Site visit data:**

This website records your visit and logs the following information for statistical purposes -your server's address; the name of the top-level domain from which you access the Internet (for example, .gov, .com, .in, etc); the type of browser you use; the date and time you access the site; the pages you have accessed and the documents downloaded and the previous Internet address from which you linked directly to the site.

We will not identify users or their browsing activities, except when a law enforcement agency may exercise a warrant to inspect the service provider's logs.

#### **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. This site does not use cookies.

#### **Email management - collection of Personal Information:**

Your email address will only be recorded if you choose to send a message. It will only be used for the purpose for which you have provided it and will not be added to a mailing list. Your email address will not be used for any other purpose, and will not be disclosed, without your consent.

If you are asked for any other Personal Information you will be informed how it will be used if you choose to give it. If at any time you believe the principles referred to in this privacy statement have not been followed, or have any other comments on these principles, please notify the webmaster through the contact us page. Note: The use of the term "Personal Information" in this privacy statement refers to any information from which your identity is apparent or can be reasonably ascertained.

*(Write topic wise details about your organisation and website)*

**4. Content Contribution, Moderation & Approval policy (CMAP) (clause 5.2.1)**

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

**5. Content Review policy (CRP) (clause 5.2.3)**

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.

**6. Content Archival Policy (CAP) (clause 10.4)**

For time sensitive content which expires after a certain date (e.g. tender notifications, announcements for conference registrations, contest entries etc.), a policy on whether the content should be archived for future reference or removed altogether from the website should be decided by the concerned Department after careful consideration of their nature of content. However, expired content MUST not be presented or flashed on the website. The Departments MUST have a clearly laid out Content Archival Policy (CAP) clarifying the rules set in this regard.

*(Write topic wise details about your organisation and website)*

## **7. Security policy (clause 7.7.2)**

### **Sample**

#### **A. Website Security Policy of XYZ**

XYZ has a responsibility to protect from disclosure to unauthorized parties the personally identifiable information (name, address, date of birth, social security number, etc.) of its website users. Therefore, XYZ has adopted and implemented a website security policy to protect account information of its website users.

#### **Notice and Disclosures**

XYZ will not sell, trade, nor disclose the personally identifiable information of its website users to any unauthorized third parties.

#### **Data Quality and Access**

XYZ takes all steps possible to ensure that the data on the website is accurate. If something is found to be inaccurate XYZ will make every effort to correct said information as quickly as possible. If it is found to be an inaccuracy with the entire system XYZ will work swiftly to correct the problem so that your web experience is as trouble-free as possible. Any change to your user account will not be reflected on the website until the following business day. The information contained on the XYZ website is subject to change without prior advance notice.

XYZ uses cookies to enhance the website experience for its registered users. A cookie is a small file that is stored on the users hard drive. XYZ uses this file to maintain certain information about the user as they move between pages. Upon closing your browser, the cookie becomes inactive and a new one will be created the next time you sign on to use one of the password protected features on the XYZ site. Most browsers are shipped to accept cookies, but this is a function that can be controlled by the user. However, many of the services offered on the website may not run optimally or at all without cookies enabled.

While using the XYZ website certain information such as your IP Address and time spent on pages may be collected. This non-personal information is collected in order to monitor any unauthorized use or access to the XYZ site. Anyone caught attempting to harm, steal information from, or otherwise damage the XYZ website will be prosecuted to the full extent of the law.

#### **Data Security**

XYZ takes security very seriously and has therefore taken every precaution to secure our borrowers information. In order to secure the users information, XYZ has implemented several security measures to prevent loss, theft, or misuse of any borrower data.

When borrowers use features on the XYZ website that involves the transferring of personal information, XYZ requires that a secure connection first be established using 128-bit Secure Socket Layer (SSL) technology. During a secure SSL session, data passed back and forth between the user's computer and XYZ's servers is secured through the use of public key cryptography. The user's computer exchanges key information with XYZ's computers to create a private conversation that only the user's computer and XYZ's systems may understand. The U.S. government regulates 128-bit encryption; it can only be used by citizens and permanent residents of the United States and Canada. To benefit from this security and to use many of the features on the XYZ site you will need to download a 128-bit enabled browser from Microsoft, Netscape, or another software company.

In addition to using 128-bit encryption in the browser, all bank account numbers that are stored in XYZ's databases are encrypted.

Each time you enter a secure connection while using the XYZ website your browser will notify you, unless the feature has been turned off. Please note that if you have left a secure connection all data sent to XYZ is over an unsecure connection.

## **Contacting US**

If you have any questions regarding the XYZ Website Security Policy, please contact the XYZ using the information below: **Write to XYZ at:**

(Write topic wise details about your organisation and website)

## **Sample**

### **B. Website Security Policy ( XYZ. Com)**

Your website represents your company in the virtual world of the internet. With any serious website, internet security needs to be considered very carefully. Zeald.com takes your website's security very seriously and provides industry standard security measures to ensure that important business information is never compromised.

#### **Physical Security**

Our servers are located in a secure hosting facility based in Northcote, Auckland, New Zealand. The building is reinforced with double-thick, cinder-block construction, top, bottom and sides.

#### **Connectivity**

The hosting facility is carrier neutral, with redundant connections from multiple providers, including Telecom, Vector Communication and TelstraClear. The hosting facility is connected via ATM and Fast Ethernet with connections directly to the Sky Tower, the Auckland Peering Exchange (APE) and upstream international providers, making it one of the most well-connected hosting facilities in New Zealand.

#### **Data Security and Back-up**

All data is located on secure servers that are continually monitored and maintained. All operating systems and applications are maintained at recommended patch levels for the highest level of operating system security possible. A full back-up of all data automatically occurs on a nightly basis and a weekly data back-up is stored off-site at a secure location.

#### **Perimeter Defense**

All servers are monitored around the clock for attempted network attacks. Industry standard Intrusion Detection Systems (IDS Systems) are employed to ensure that any breach of the perimeter defense is detected and dealt with immediately.

#### **System Redundancy**

The cluster of servers that provides all Zeald.com systems and tools is designed for 24 x 7 x 365 operations. Complete redundancy is built-in at every point, including disk arrays and redundant web, database and file servers.

#### **SSL Data Transmission Security**

The highest level of SSL browser encryption is used to ensure that all sensitive data transmissions between your customers and your website are encrypted and secured to the highest level possible.

(Write topic wise details about your organisation and website)



**Sample**

**C. Website Security Policy (North Dakota Legislative Council)**

The State of North Dakota uses secured servers for conducting online transactions. It has taken a number of steps to XYZeguard the integrity of its data and to provide reasonable protection of private information that is in our possession. All credit card and other payment information that is transmitted is protected by 128-bit encryption technology using Secured Socket Layer (SSL) protocol, provided the website user's browser is properly configured and the user's computer is operating properly.

For information security purposes, the computer systems that host discoverõ õ õ õ õ com and other state websites employ software programs to monitor network traffic to identify unauthorized attempts to compromise its devices. If security monitoring reveals possible evidence of criminal activity, information pertaining to such activity may be provided to law enforcement officials

**Sample**

**D. Security Policy (Private company)**

**Purpose of Policy**

This policy addresses the measures taken to XYZeguard the integrity of the County of Sutter's (County) network and computing infrastructure, including but not limited to monitoring, auditing, and encryption.

**Policy Contents**

The following sections of our Website Security Policy explain these uses:

- A. Security Measures
- B. Site Monitoring

**A. Security Measures**

Security measures have been integrated into the design, implementation, and ongoing practices of the entire County operating environment as part of its continuing commitment to risk management.

For sensitive information such as that requested on the -----Form, users connect to the County website via a secure network protocol (SSL), and user information is transmitted through secure lines (encrypted data) to a departmental database. This database may retain, if provided, personal information that could potentially be used to identify individual users (e.g., e-mail address, phone number, etc.).

Any technical standards governing security are enforced by the County's Information Technology Department. Under no circumstance should this policy be construed as warranting as fail-proof the absolute security of information provided and gathered through County supported websites.

Please refer to the XYZ Privacy Policy for more information regarding the collection and XYZ safeguarding of information.

**B. Site Monitoring**

The County provides this website and the information it contains as a public service. This system is monitored to ensure proper operation, to verify the functioning of applicable security features, and for comparable purposes. Anyone using this system expressly consents to such monitoring.

Unauthorized attempts to modify any information stored on this system, to defeat or circumvent security features, or to utilize this system for other than its intended purposes are prohibited and may result in criminal prosecution.

(Write topic wise details about your organisation and website)

## **C. Responsibility and Authority (website management team):**

### **1. Web Information Manager (clause 10.1.1)**

Appointed by the Ministry, whose role shall be to ensure that there is a proper flow of content to the site and that content quality and user satisfaction issues are taken care of. To achieve this he has to coordinate with the various groups within the department/ministry. The Web Information Manager should undertake the following activities with regards to the website being maintained by him.

- Formulation of policies concerning management of content on the web through its entire life cycle viz. Provision, Moderation Approval and Archival. Ensuring that all content on the website is always authentic, up-to-date and obsolete information or services removed.
- Changing and periodically validating links to related information. An automated report can provide a list of broken links on the site, which can be immediately corrected.
- Ensuring the entry of the website at a prominent rank in all the major search engines so that the site's visibility is enhanced and users are made aware of its address.
- Web Information Manager is overall responsible for quality and quantity of information and services on the website. The complete contact details of the web Information manager must be displayed on the website, so that the visitor could contact him/her in case of some queries or requirements.
- Since the websites receive a lot of feedback mails from the visitors, it is responsibility of the Web Information Manager to either reply to all of them himself/herself or designate someone to regularly check and respond to the feedback/query mails.

### **2. Technical Manager (optional )**

He should also be appointed (or outsourced) for every website owner whose responsibilities would be:

- Regular monitoring of website for Performance, Security and Availability
- Ensuring compliance with policies (organizational, regulatory, legislative, etc) that may require changes in website content, architecture, security, process etc.
- Periodic security audit of the website in line with major revisions
- Analysis of traffic on website and feedback to development / management team

In case of a large website / multiple websites, a team should be set up with web information manager having professionals skilled in HTML authoring, programming, design, content etc. This team must also draft content management (provision, moderation & approval) and archival policies with regard to each section in the website.

The Technical Manager should have a experience and skill in the following knowledge areas:

- Website Technology
- Website Testing
- Usability
- e-accessibility
- Performance
- Security
- Guidelines for Indian Government websites
- Content Management System

(Write topic wise details about your organisation and website)

## **D. Plans:**

### **1. Contingency plan in the event of defacement/ natural calamity (clause 8.3)**

The website of a Government Department is its presence on the Internet and it 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 minimize 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. The possible contingencies include:

**Defacement of the website:** All possible security measures MUST be taken for a Government website to prevent any possible defacement/hacking by unscrupulous elements. However, if despite the security measures in place, such an eventuality occurs, there must be a proper contingency plan, which should immediately come into force. If it has been established beyond doubt that the website has been defaced, the site must be immediately blocked. The contingency plan must clearly indicate as to who is the person authorized to decide on the further course of action in such eventualities. The complete contact details of this authorized person must be available at all times with the web management team. Efforts should be made to restore the original site in the shortest possible time. At the same time, regular security reviews and checks should be conducted in order to plug any loopholes in the security.

**Data Corruption:** A proper mechanism has to be worked out by the concerned Government Departments, in consultation with their web hosting service provider to ensure that appropriate and regular back-ups of the website data are being taken. These enable a fast recovery and uninterrupted availability of the information to the citizens in view of any data corruption.

**Hardware/Software Crash:** Though such an occurrence is a rarity, still in case the server on which the website is being hosted crashes due to some unforeseen reason, the web hosting service provider must have enough redundant infrastructure available to restore the website at the earliest.

**Natural Disasters:** There could be circumstances whereby due to some natural calamity, the entire data center where the website is being hosted gets destroyed or ceases to exist. A well planned contingency mechanism has to be in place for such eventualities whereby it should be ensured that the Hosting Service Provider has a Disaster Recovery Centre (DRC) set up at a geographically remote location and the website is switched over to the DRC with minimum delay and restored on the Net.

Apart from the above, in the event of any National Crisis or unforeseen calamity, Government websites are looked upon as a reliable and fast source of information to the public. A well defined contingency plan for all such eventualities MUST be in place within all Departments/organizations so that the emergency information/contact help-lines could be displayed on the website without any delay. For this, the concerned person in the Department responsible for publishing such emergency information MUST be identified and his/her complete contact details should be available at all times.

(Write topic wise details about your organisation and website)

## 2. Website Monitoring plan (clause 10.3)

Websites must be monitored periodically in accordance with the plan to address and fix the quality and compatibility issues around the following parameters:

**Performance: a.** Site download time should be optimised for a variety of network tested for this.

**Functionality: b.** All modules of the website should be tested for their functionality. Moreover, interactive components of the site such as discussion boards, opinion polls, feedback forms etc. should be working smoothly.

**Broken Links: c.** The website should be thoroughly reviewed to rule out the presence of any broken links or errors. A number of tools and techniques are now available to easily detect the broken links in a website

**Traffic Analysis: d.** The site traffic should be regularly monitored to analyse the usage patterns as well as visitors profile and preferences. Traffic Analysis tools also give reports on broken links.

**Feedback: e.** Feedback from the visitors is the best way to judge a website's performance and make necessary improvements. A proper mechanism for feedback analysis should be in place to carry out the changes and enhancements as suggested by the visitors.

(Write topic wise details about your organisation and website)



**E. Organisation Structure**

- 1. Website developer**
- 2. IT service provider**
- 3. Content management**
- 4. Data center / Hosting organisation**
- 5. User**
- 6. Application Developer**

## Compliance statement

### 1. w.r.t. Guidelines for Indian Government Websites 2018 (refer Annexure - I attached)

- I hereby state that our website complies fully with the Guidelines for Indian Government websites.
- I hereby state that our website complies with the NIC Guidelines for Indian Government websites.

-- Signed & stamped by Web Information Manager --

### 2. Security Audit report (clause 7.7.1)

The security audit of our website at URL  .  
Hosted by  .. . and managed by  ..  
has been audited by  ..  
and no major non. conformity observed.

Report number:  . dated: ..

Enclosed: Copy of valid Security Audit Certificate

-- Signed & stamped by Web Information Manager --

**H. Miscellaneous:**

**1. Person responsible for updating of website quality manual**

Web Information Manager is responsible for updating the website quality manual. He collects information ò ò ò ò ò ò ò ò ò ò ò ò ò ò ò ò ò .

**Compliance Matrix**  
**Guidelines for Indian Government Websites 2018 - Criteria**

No.	GIGW Requirement	Ref. No.	Status/ Remarks
	<b>1. General Guidelines</b>		
1	Department has nominated a Web Information Manager as defined in the guidelines	10.1.1	
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 web site.	9.2.1 & 9.2.2	
3	Website has the following clearly defined policies and plans approved by the web information manager ó 3.1.1 - Copyright Policy. 5.2.1 - Content Contribution, Moderation & Approval (CMAP) Policy. 10.4 - Content Archival (CAP) Policy. 5.2.3 - Content Review (CRP) Policy. 3.2.1 - Hyper linking Policy. 3.4.2 - Privacy Policy. 3.3.1 -Terms & Conditions. 10.3 - Website Monitoring Plan. 8.3 - Contingency Management Plan. 7.7.2 - Security Policy.	10.7	
4	Source of all documents, not owned by the dept. that have been reproduced in part or full, is mentioned.	3.1.5	
5	Due permissions have been obtained for publishing any content protected by copyright.	3.1.4	
6	Home page of website displays the last updated/reviewed date.	5.2.2	
7	Complete information including title, size format and usage instructions is provided for all downloadable material.	4.4.7(a), 6.7.1(a), 6.7.1(b)	
8	With respect to each, Circular, Notification, Document, Form, Scheme, Service and Recruitment notice, the following should be clearly listed in the Website: Complete Title Language (if other than English) Purpose/ Procedure to apply (as applicable) Validity (if applicable)	4.2.3 (a,d,e), 4.2.4 (b,d), 4.2.5 (b,c), 4.2.6 (c,e,f), 4.2.7 (a,d), 4.2.9 (a,b,d)	
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.	5.2.6	

No.	GIGW Requirement	Ref. No.	Status/ Remarks
10	The language is free from spelling and grammatical errors.	5.3.5	
11	Mechanism is in place to ensure that there are no -broken linksø (internal as well as external) or -Page not foundø errors.	3.2.9	
12	There are no links to -under constructionøpages.	6.8.4	
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.	3.2.8 & 3.2.5	
14	Website provides a prominent link to the -National Portalø from the Home Page and Pages belonging to National Portal load in new browser window.	2.3.1 & 2.3.2	
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.	2.1.1, 6.3.1, 6.1.1	
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.	2.1.2 & 6.8.5	
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.	7.2.1	
18	Website is readable even when style sheets are switched off or not loaded.	7.2.2	
19	Proper page title and language attribute along with metadata for page like keywords and description are appropriately included.	7.5 (k), 9.1.2	
20	Data tables have been provided with necessary tags/ markup.	7.5 (l)	
21	The website has a readily available Help section linked from all pages of the website.	4.4.6	
22	All information about the department, useful for the citizen and other stakeholders, is present in the -About Usø section and mechanism is in place to keep the information up to date.	4.2.1	
23	Website has a -Contact Usøpage 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.	4.2.11 (a) & 4.2.11 (c)	
24	Feedback is collected through online forms and mechanism is in place to ensure timely response to feedback/queries received through the website.	4.4.5(a), 4.4.5 (c)	

No.	GIGW Requirement	Ref. No.	Status/ Remarks
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).	6.4.3, 7.6 (b)	
26	Minimum content as prescribed in the guidelines is present on the homepage and all subsequent pages.	4.5.1, 4.5.2	
27	It is ensured through Content Moderation and Approval Policy that website content is free from offensive/discriminatory language.	4.7.2	
28	Text is readable both in electronic and print format and the content prints correctly on an A4 size paper.	6.4.6	
29	Website has cleared security audit.	7.7.1	
30	Website is in the nic.in or gov.in domain.	2.2.1	
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.	8.2.1 (a, b, c, d & h)	
32	Website is bilingual with a prominent language selection link and uses unicode characters.	5.7.1	
33	Documents/Pages in multiple languages are updated simultaneously.	5.7.2	
34	Documents are provided either in HTML or other accessible formats. Download details (File Format Size) & instruction for viewing these is provided.	7.4.2 (a)	
35	Mechanism is in place to ensure that all tender/recruitment notices are published/ linked through the website.	4.2.8, 4.2.9	
36	All documents have a publish date on the main page.	5.2.5	
<b>Accessibility Guidelines</b>			
1.	All non-text content (like images) has a text alternative that provides equivalent information as the image itself.	6.6.3	
2	Scanned Images of text have not been used.	6.6.1	
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.	6.5.1	
4	Text can be resized without assistive technology up to 200 percent without loss of content or functionality.	6.4.5	

No.	GIGW Requirement	Ref. No.	Status/ Remarks
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.	6.7.3 (b)	
6	Web pages do not contain any content that flashes for more than three times in a second.	6.7.3 (a)	
7	Instructions provided for understanding and operating content do not rely solely on sensory characteristics such as shape, size, visual location, orientation, or sound.	7.5(d)	
8	Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	6.5.4	
9	Captions or transcript are provided for all prerecorded and live audio and video content.	6.7.2 (a, b)	
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.	6.7.3 (c)	
11	Information, structure, and relationships that are conveyed visually on a web page must also be programmatically determined or are available in text.	5.6.3	
12	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	5.6.4	
13	All functionality that is available on the web page is operable through keyboard.	7.5 (f)	
14	Complete web page is navigable using keyboard only (using tab or arrow keys).	7.5 (g)	
15	Current navigation location (Keyboard focus indicator) is visible on the webpage while operating or navigating the page through a keyboard.	7.5 (o)	
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).	6.8.8	
17	Any web page within the website is locatable either through search or a sitemap.	6.9.1, 6.10.1	
18	Navigational mechanisms that are repeated across the website occur in the same relative order on each page.	6.8.2, 6.2.1	

No.	GIGW Requirement	Ref. No.	Status/ Remarks
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).	7.5 (m)	
20	The purpose of each link is clear.	7.5 (h)	
21	Time limit for time dependent web functions is adjustable by the user.	7.5 (c)	
22	Complete & self-explanatory title that describes the topic and purpose of the page has been provided.	2.1.6	
23	Headings wherever used, correctly describe topic or purpose of content.	5.6.1	
24	Language of the complete web page has been indicated. If there is a change in language within a webpage it also indicated.	5.3.7	
25	Nomenclature of components that have the same functionality is uniform across the website.	5.4.2	
26	When any component on the web page receives focus or its settings are changed it does not initiate change in context.	7.5 (j)	
27	Changing the setting of any user interface components does not automatically cause a change in context.	7.5 (i)	
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.	7.5 (p), 7.5 (e)	
29	Labels or instructions have been provided wherever input from the users is required.	7.5 (b)	
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.	7.5 (q)	
31	Web Page uses markup language as per specification.	7.5 (a)	
32	Name and Role of all interface components can be programmatically determined.	7.5 (n)	