Shri C. J. Venugopal, IAS
Principal Secretary to Government
& Chairman, OCAC

Government of Odisha
Electronics & Information Technology Department
OCAC Building, Plot No.N-1/7-D, Acharya Vihar
Bhubaneswar-751013, Odisha, India
Ph. No.: + 91-674-2567584 (O), Fax : + 91-674-2567842
Website : www.ocac.in, e-mail : itsec.or@nic.in

No 206 /E&IT Dated 24/01/2019

To

All Additional Chief Secretaries to Government/
All Principal Secretaries to Government/
All Commissioner-cum-Secretaries to Government/
All Heads of Departments

Sub: Guidelines on Websites & Portal development, Hosting and maintenance.

Ref: No.441/IT dated 15/02/2016

Sir,

In inviting a reference to the subject cited above, I would like to intimate that all sites/portals developed for Government of Odisha must adhere to the Guidelines for Indian Government websites (GIGW), ISO 23026, W3C's Web Content Accessibility Guidelines (WCAG 2.0), Rights of Persons with Disabilities Act 2016 and Information Technology Act, 2000. In this regard the detailed guidelines for design, development, hosting and maintenance of websites/ portals has been prepared by E & IT Department.

All departments are requested to adhere to the guidelines for design, development, hosting and maintenance for websites/portals and take suitable action.

Yours' faithfully,

Principal Secretary to Government

Electronics and Information
Technology Department
Government of Odisha

GUIDELINE
ON
WEBSITE AND PORTAL DEVELOPMENT, HOSTING AND MAINTENANCE

Electronics & Information Technology Department,
Govt. of Odisha

Contents

1. OBJECTIVE 3
2. INTRODUCTION 3
3. Guideline for Website Design and Development 4
3.1. Design, Development of Websites 5
4. Guidelines for Content Development and Administration 6
5. Guideline for Departmental Application Integration 8
5.1. Presentation-level integration 8
5.2. Business Process–Level Integration 8
5.3. Data-Level Integration 8
5.4. Communications-Level Integration 9
5.5. Security Measures to be taken during Integration 9
5.5.1. Security Policy 9
6. Guideline for websites updating and maintenance 10
7. Guidelines for Domain Name convention and Registration 10
8. Guideline for Hosting websites 11
8.1. Contingency Management 12
8.1.1. Defacement of the website: 12
8.1.2. Data Corruption 13
8.1.3. Hardware / Software Crash 13
8.1.4. Natural Disasters 13
8.1.5. Hacking monitoring system 14
9. Guideline for security of websites 14
10. Guidelines for website and domain administration 15
11. Guidelines for website promotion and marketing 15
12. Legal framework 16
13. Reference links 16

1. OBJECTIVE

This document supplements the "Guidelines on Dissemination of Information through Government Websites". It highlights some useful technical information and good practices in developing websites for reference by Government departments, to enable effective, efficient, and user friendly dissemination of information through websites.

To formulate an integrated approach to build a knit and secured cyber presence for the State Government, this gives an impetus to the preparation of a policy for the Website Development, Hosting and Maintenance for various State Government Departments, line offices, Boards, Agencies, Boards, and Corporations etc.

2. INTRODUCTION

Businesses, world over are leveraging on the potential of Internet as a mass media and are using it to communicate with their clients. These users or citizens are also expecting the Governments to perform in a similar fashion and thus expect to get the latest and up-to-date information about any change in Act, Rule, Regulation, all new Notifications, Circulars, activities, events, schemes, services etc. from its web site at the click of mouse. However our websites are riddled with the problems of obsolete and old content as well as the absence of desired content. Sensitization of the concerned persons towards the need for timely and up-to-date information on the web is extremely important. Therefore it is suggested that a well defined strategy may be worked out within the Department, offices, and other Government establishments to ensure timely provision of content to be posted on the website. There should be clear understanding within the organization about where the responsibility lies for providing content for the website, and in what form it should be presented to the web team.

Government of Odisha emphasizes on usage of Web Technology to disseminate the information across the globe and to enhance the Citizen-Government interface by bridging the digital divide. Departments and their subordinate offices develop their websites (Web Applications also) at their end to cater the needs. They develop the websites using different tools and technologies. The process of developing organization specific websites has also started and a number Departments, Boards and Corporation and district authorities have made their web presence. However most websites are riddled with the problems of obsolete and old content as well as the absence of desired content, security etc.. Sensitization towards the need for timely and up-to-date information on the web, security of content and data, management of websites and portal are extremely important. Therefore a well defined strategy needs to be worked out to ensure timely provision of content to be posted on the websites, ensure security of the websites and management of website. There should be clear understanding within the organization about where the responsibility lies for providing content for the website, and in what form it should be

presented to the web team, how security of the website can be assured, how websites can be managed and monitored.

3. Guideline for Website Design and Development

With the ever-growing reach of the Internet to public day by day, it has become an easy, fast and effective way of reaching out to the people. Every Government organization or Department which has to deal with public or which has to disseminate information to masses now a days opt for putting all the relevant information on the web because of following advantage.

a. **Universal Accessibility** – The Website/Portal should be accessible to all irrespective of Technology, Platforms, Devices or Disabilities of any kind. In other words, the needs of the broad spectrum of visitors like general public, specialised audiences, people with disabilities, those without access to advanced technologies and people with limited English proficiency should be considered.

b. **Fast Loading** –No one wants to wait (and wait and wait) for your site to load. Design sites with prompt loading times for all users on all devices (even the ones with slower Internet connections). It also helps for Easy and fast access to the required information.

c. **Mobile Ready**–Virtually everyone uses smart devices on a daily basis. Create an engaging, mobile-friendly design that your audience can access whenever they want, wherever they roam.

d. **Tracking Enabled**–The best way to determine that,the website is actually doing its job, the final design should include functionality to gauge key indicators such as traffic, goals, and conversions.

e. **Enabled CMS**–Consistently publishing fresh, original content not only captivates the audience, it can deliver invaluable, long-term digital marketing momentum. Include a back-end Content Management System in the design to post and edit content as needed.

f. **Conversion Optimized** –Implement tools for creating campaign-landing pages. These designated pages can keep your readers moving through your site for their relevant work. It helps in less rush in the offices& increase efficiency in replying to the public queries.

g. **Social Media**–Integrate all relevant social media platforms within your design. Allowing users to quickly access social media pages from the website instantly and helps increase visibility. It also helps for reaching Globally &Increase the popularity.

h. **Strong Security**–Every design should include fundamental security and privacy protocols, such as basic security checks, to protect data. Periodical Security Audit of web applications need to be done on regular basis.

i. **Cost efficiency** –Ease of use, support for a variety of content, automated templates, content workflow management are some of the features to be looked into in CMS software. For small scale websites, developers could also develop website specific CMS solutions, as it may turn out to be cost effective in many instances.

j. **More attractive way to advertise itself** -It has been ensured that all stationery of the department as well as advertisements/public messages issued by the concerned Department prominently display the URL of the web site. The more the website will be attractive, the more it will advertise itself.

k. **Public awareness**–All the public awareness campaigning should be incorporated in the departmental websites as and when required. Mobile platform may also be used for Public awareness campaigning.

3.1. Design, Development of Websites

a) The Department/Line offices, other Government organization may develop their websites on their own or by engaging external agencies. Irrespective of who develops the website the Layout of the site and design the entire web site/Portal should be as per the Guideline for Indian Government Websites (GIGW), International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines (WCAG 2.0), Rights of Persons with Disabilities Act 2016 as well as Information Technology Act of India and latest Open Web Application Security Project (OWASP) Developer Guideline.

b) The site map shall be prepared and duly approved by the Head of the Organization. The Design shall be approved by concerned HOD/Secretary of Administrative Department.

c) A uniform pattern may be maintained so as to give an integrated look about State of Odisha. The Website/Portal should be developed in Bilingual form (English & Odia) and should be disable friendly. Unicode should be used for development of website

d) The website should be developed on the platform which is most secured and available in Hosting Environment. For Example LAMP, WAMP etc.. The development of web portal may preferably be done in open source/platform.

e) The Website and apps should be designed and developed in such way that they are accessibleby all people, whatever may be their hardware, software, language, culture, location, or physical or mental ability.

f) If any service is delivered online then it should be developed as a web service so that other websites and portals can access it seamlessly, subject to authorisation of the owner Department. All online services should be made available through the Government Portal.

g) All documents developed/published and issued in the Public Domain by Government Departments must be published on the website. This content should be reviewed regularly to ensure the accuracy and currency of the information. The complete official title and date of the document MUST be mentioned on the website. The correct title would lead to an accurate search output for that document and it would be easy for the users to locate it. In case any reference to a document of another Government Department is given, it should be clearly specified as with whom

lies the ownership of the document. The document should be bilingual. Documents must be made available in an accessible format.

4. Guidelines for Content Development and Administration

a) The web content is entirely different from that of the print and audio-visual media and needs special care for drafting. The web content can serve multiple purposes and can be both brief as well as detailed. The Website content should be develop to enable maximum public interface and it should facilitate the citizen of the state in getting information about various scheme, procedure, policies and rules & regulation of the Government.

b) For the content development, the site maps for navigation of the site is the first and foremost requirement and should be prepared in the first place. The concerned officer of the Department or office as per the approved site map should prepare the content pertaining to the links. The contents for the Departments/offices should be approved from the concerned Secretary/ Head of the Organization before handing it over to the Website designing team for designing the website.

c) When users navigate sequentially through content, they should encounter information in an order that is consistent with the meaning of the Content Development for Government Apps & Websites and can be operated from the keyboard. Hence if a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components MUST receive focus in an order that preserves meaning and operability.

d) Department/District/other offices shall engage a Content Administrator for the websites managed by them. His name, designation, e-mail id and telephone number should be made available to the webmaster of the website/portal. Any change in name/designation must be immediately informed to the webmaster.

e) Content Administrator shall approve the contents of the Website of the Department/office and a communication will be sent to concern person, before hosting it on the Website. Any change, whatsoever, to be made in the Official Website of the Department/office shall be first reported to Department/office Head and after obtaining his approval, the necessary changes should be made in the website.

f) The Content Administrator shall be responsible for timely forwarding of the information for uploading on the website and shall ensure that no information should be forwarded for uploading on private websites.

g) The Content Administrator shall clearly mention whether to place the information in the public domain or department domain..

h) Content Administrator shall ensure that all the information forwarded by him should be in soft copies only i.e. e-mail, CD, DVD. The data should be provided preferably in doc format. Scanned documents and files in pdf format, jpg format etc. may be avoided.

5. Guideline for Departmental Application Integration

Application integration means helping a series of applications communicate with one another better. To ensure that the integration is both beneficial and feasible, however, it should closely examine the business processes that must be integrated before focusing on the applications themselves. If the business processes of the organization uses is understood, then it can map those processes to the application integration requirements.

Application integration can occur at many different levels, including:

- Presentation level
- Business process level
- Data level
- Communications level

5.1. Presentation-level integration

Presentation-level integration can be a very effective way of integrating applications in an environment. Presentation-level integration allows multiple applications to be presented as a single cohesive application, often using existing application user interfaces.

5.2. Business Process–Level Integration

Before designing the application integration environment, it is important to understand the organization in logical terms, removed from the technology that underlies it.

Business processes consist of a group of logical activities that model the activities in the organization. These activities typically represent the smallest units of logical work that can be done in the organization. Business processes usually have a beginning and an ending state, and generally have action-oriented names. When the order is processed, it goes from an unprocessed state to a processed state. The order-processing rate can be measured to show the efficiency of the process.
Any applications that are related in a given business process are candidates for integration. The reason for integrating the applications is to help the business process in some way; by making it faster, less error-prone, or less expensive.

These dimensions define the complexity of the business process. They also drive the complexity of the integration of IT services in terms of whether the IT service is available at that place and time, and whether the service has the necessary business process state information. The complexity of the business process can also be affected by the nature of the applications involved in integration; for example, their maturity, degree of integration, and so on.

5.3. Data-Level Integration

Applications to communicate with each other at a business process level, they need to understand the data they exchange. Because different applications often handle data in different ways, a number of capabilities are required to establish integration at the data layer.

There are two general ways to enable data-level integration:

- Add logic to enable each application to understand incoming data from other applications.

- Add logic to enable each application to interpret outgoing data to an intermediate data format and interpret incoming data from that format into a form the application understands.

In most situations, application integration architecture should instead adopt the second approach, with the data level using an intermediate data language.

Different integration scenarios have different data-level requirements. The nature of the applications integrated, may alter the way in which the data capabilities can function. The data capabilities must normally be small, quick, and multithreaded. Other applications may only need to transfer data in batches. The data may need to be particularly strong at sorting, summarizing, and filtering sets of data.

To support the various complex data integration requirements, the application integration solution must often contain a considerable amount of logic that supports the access, interpretation, and transformation of data. It also needs schematic models of data to describe data attributes. The definition and recognition of schemas enables the validation of data.

5.4. Communications-Level Integration

All the forms of integration already discussed are depend on integration at the communications level. Not all applications are designed to communicate in the same way. Some communicate synchronously, others asynchronously. Some use file transfer to communicate; others interact through messaging or request/reply.

The nature of the applications integrated often determines how communications occur between them. Older applications may use file transfer for communications. Newer applications often use message-based communication and may use predefined standards to facilitate communication. Before determining the requirements for the communications-level integration, it needs to examine the communication needs for the environment and the existing capabilities of the applications.

5.5. Security Measures to be taken during Integration

A well-designed application integration environment rapidly becomes an integral part of the organization. Therefore, security vulnerabilities in application integration have the potential to cause wide-ranging problems. Operational practices must be well-defined so that the application integration environment can continue to operate effectively and reliably over time.

5.5.1. Security Policy

The first step toward effective security in any environment is creating a written security policy. Many factors can affect the security policy, including the value of the assets to be protected, the threats that the environment faces, and the vulnerabilities that are currently present. The security policy should form the basis of any security measures that takes in the organization. Before making modifications to the environment, it should be ensured that, they are consistent with the security policy. The policy should be examined itself periodically to determine whether it needs to be redefined in the wake of new business requirements and to verify that the procedures and standards that implement the policy adhere to industry best practices.

Note: - Security audit must be done for the entire system after application integration takes places. Please refer to Clause 9 in this regard.

6. Guideline for websites updating and maintenance

Once the website is Go-Live, regular update and maintain the website is the responsibility of the user Department/Office. The Department/Officemay hire a suitable Agency for the same or do it by their own. However, following checklist may be followed for update and maintain their website:

a) Thoroughly review and test the entire website (periodically).

b) Test the website forms/checkout process(periodically).

c) Review the KPIs, SEO (Search Engine Optimization) and analytics reports on a regular basis.

d) Security updates and bug fixes periodically or as patches are released.

e) Renew website domain name (annually).

f) Check backups on a regular basis.

g) Test browser compatibility on a regular basis.

h) Update dates and copyright notices periodically.

i) Review contact information (periodically or as needed).

The updating of the official websites shall be done through the agencyengaged or the technical team engaged for updating through a secured connection to the hosting environment, preferably through SSL VPN. The departments shall identify one nodal officer who will be responsible for authentication and updating of the website in respect of their organization.

7. Guidelines for Domain Name convention and Registration

Domain Name Convention:

a) The Domain name for the website should be coined in such a way that state identity is visible in the name besides department or office identity.

b) The Domain Name for websites or portal of Government Departments and Offices must be under GOV.IN domain.

c) The line offices of the departments and other associated bodies should have domain name at 4th level under the concerned Department's Domain.

d) Districts must have domain name under GOV.IN

e) Other offices like state PSUs may have their website under .IN domain or NIC.IN domain (like IDCO may have website domain name IDCO.NIC.IN or IDCO.IN).

f) The domain name must be approved by the Administrative Department and informed to E&IT Department for its record and reference.

Domain Name Registration and Control

a) Registration for .GOV.IN may be done online through the website www.registry.gov.in .However off line registration is also possible.
b) Registration for .NIC.IN may be done through NIC (http://nicregistry.nic.in/).
c) In order to get the registration done quickly, the ink signed copy of authorization letter may be sent to Domain registrar through Fax and speed post. Alternately authorization letter may be sent to Website coordinator of NIC.
d) The Name Server for Domain shall be from Government Internet Service Provider (ISP). Private ISPs shall be avoided as Name Server provider.
e) At least two Name Servers from different ISPs should be selected for high availability.
f) The domain names are generally registered with an Administrative, Billing and Technical Contact. The ownership remains with the Department/person having the Administrative and Billing rights. However, the Technical Contact remains with the organization maintaining the Web Server on which the Web site is hosted. It has generally been noticed that Departments/offices getting their domain name registered through third party service provider do not know this aspect and the ownership remains with the third party service provider. It is the privilege of the Administrative/Billing rights holder to keep/maintain any content on the web site. The Departments/offices getting the domain registered through some other service provider organization will have no control and ownership right on the web site. It is therefore essential that the ownership of the Web site should remain with the concerned Department/office rather than any third party through which the site has been registered. Since, adequate technical manpower is not available in most of the Departments, Boards and Corporations; it is difficult to address this issue independently by the State Government Organizations. Accordingly, in order to address this issue properly, it is essential to keep track of the Ownership Rights and Technical Control issue. Therefore, the ownership of the Departmental websites domain names shall remain with the E&IT Department and the ownership of other portal sites having independent domain names shall remain with concern organization.
g) The Registrant, Administrative Control and Technical Control officers should have eMail ID either in .GOV.IN or .NIC.IN domain (i.e. adminpr@nic.in or adminpr@odisha.gov.in etc.)
h) The Department/offices wishing to register domain name (GOV.IN) through E&IT Department are required to apply in the prescribed format (annexure-1). However, all are free to register their domain name at their end. In case the Department/office registers its domain name on its own, it has to inform E&IT Department the details of the Domain as per format given as annexure-2.
i) The Departments those are having already registered domain names should intimate the details as per annexure-2 to E&IT Department forthwith.
j) The Departments and/or its line offices that are having their domain name registered under different domain other than .GOV.IN should immediately register a domain name in .GOV.IN.

8. Guideline for Hosting websites

a) It is quite vital to host the website and portal in such an environment where theft and loss of data are minimal or zero. Further the hosting environment should have network and

gateway security in place along with proper back up policy and DR setup. At least the environment should assure Reputation Service, Community Defence, Bot Protection, Account Takeover Protection, Fraud Prevention and certified accordingly.

b) The website must be hosted is state-of-the-art multi tier security infrastructure at both, physical and network level as well as security policies to ensure the best possible security to Government websites.

c) The Hosting Environment MUST also use devices such as firewall and intrusion prevention systems to make the website more secure. The Hosting Environment MUST have a redundant server infrastructure to ensure fastest restoration of the website in the event of any unforeseen hardware/software failure.

d) The Hosting Service Provider (HSP) should also provide the facility of staging infrastructure in order to facilitate the testing of the new websites as well as their enhanced or revised versions' content prior to publishing on the internet.

e) Provision should be given to the concerned Department to remotely update their website in a secured manner with proper ownership of the Department.

f) In view of this the Government websites/portals should be kept in Government IT Infrastructure establishments like State Data Centre/National Data Centre, STPI or any Government setup/cloud complying with Data Centre Standards.The hosting of the website/portal should be in multi-tier security zone after proper hardening/simulated testing.

g) The websites of department/offices which are already available on private IT infrastructure should immediately be moved to Government facilities.

h) Before making a request to move the website to Government facility, the department or office should ensure that the security audit has been performed and **safe to host** certificate has been obtained on latest version of their respective website/portal.

i) The Implementing Agency may provision IPv4 & IPv6 compliance during hosting of the website. If required, Dual Stack Support, i.e. both IPv4 & IPv6, must be enabled.

j) The direct IP based hosting should be avoided.

8.1. Contingency Management

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. The possible contingencies include:

8.1.1. 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 be executed. 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 authorised to decide on the further course of action in such eventualities. The complete contact details of this authorised 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 gaps in the security.

8.1.2. 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 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.

8.1.3. 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.

8.1.4. Natural Disasters

There could be circumstances wherein due to some natural calamity, the entire data centre 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 wherein 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 Web.

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

8.1.5. Hacking monitoring system

Department/Offices may implement a hacking monitoring system to protect their website proactively. They may do it through web traffic monitoring or may engage a third party agency to monitor.

TheDepartment/Offices & the Website Implementing Agency must define their **Escalation Matrix** for better communication & resolution of issues raised.

9. Guideline for security of websites

It is very vital to have a secured web presence. Hence the Websites/Portals have to be thoroughly audited and hosted on public domain. Following process shall be followed by the Departments, its line offices, districts, and other offices. All possible security measures must be taken for a Government website to prevent any possible defacement/hacking by unscrupulous elements.

All websites or web applications should follow National Cyber Security Policy.http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf.

a) The website after Development shall be audited for fixing the security lapses. The Security audit can be done either through any CERT-IN empanelled firms by adapting Government Process or through STQC. In addition, in case application is hosted or planned to be hosted in NIC Infrastructure, security audit may be done by NIC and "Safe to Host" certificate need to be obtained from NIC.

b) The website/Portal may preferably be hosted under HTTPS protocol. However it is mandatory for transactional & Intranet based web sites or applications to be hosted under HTTPS protocol.

c) Website should run independent of IP Address. i.e. IP Addresses should be not be hard coded in the source code/configuration .

d) The security audit should be done at least once in a year. However in cases where there is modification in the code of the website, the security audit should have been done before making it public.

e) Active websites must be security audited immediately, if not done.

f) A copy of "Safe to Host" Certificate should be communicated to E&IT Department in each case.

However, if despite the security measures in place, such an eventuality occurs, there must be a proper contingency plan, which should immediately be executed. 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 authorised to decide on the further course of action in such eventualities. The complete contact

details of this authorised 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 gaps in the security.

A proper mechanism has to be worked out by the concerned Government Departments, in consultation with their web hosting service provider, to ensure 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.

10. Guidelines for website and domain administration

a) The Concerned Department, District, and other offices will have to designate an officer as Web Administrator for the website/portals. He/She shall be responsible for overall management of Websites/portal. Any change in web-policy shall be approved by him/her. The broad activities of Web Administrator involves oOnline or off line registration of domain names (optional)oAdministration of Domain details i.e. Renewal of domain name, change in name server (if required), Contact updating etc.
    - Overall management of websites.
    - Coordination among webmaster, content administrator, technical team.

b) Line offices have to request the Web Administrator of the concerned Department for registration of the domain with approval letter from the authority.

c) Departments/Districts/other offices may engage Nodal officer/Administrator who shall be responsible for overall supervision to ensure that authentic and updated information is available on the website.

d) The Webmaster shall accept mail from concerned Content Administrator only and after satisfying himself about the origin and Authenticity of content shall forward such e-mail to uploading team for immediate uploading on website so that up-to-date information is available on the site.

e) Webmaster shall forward all the feedback/complaints/grievances received through email from public to concerned department so that necessary action as required can be initiated.

f) Data backup, system logs and change logs etc shall be kept at least for two years

g) Updating on the Server should be done through secured channel preferably through SSL VPN.

11. Guidelines for website promotion and marketing

Since, Web is a medium for promotion and marketing of various products and services as well as for dissemination of the information, proper marketing and promotion of these websites become extremely important so as to reach the target audience. The responsibility of marketing and promotion of these Websites shall be the responsibility of the concerned

department/organization. The organisations, concerned, shall promote the site through paper or television advertisements , the address of the website/portals shall be provided on the letterhead of concerned Organization, and any other means as decided by the authority.

a) All the advertisements/public messages including Press Releases, Tender Notifications etc. issued in the Newspapers/Audio-visual media by the concerned Department MUST prominently mention the URL of the web site clearly in order to give it due publicity. It should be directed that no press release or advertisement of any Government Department shall be issued to the press without checking the presence of the URL of the website and necessary steps should also be taken to ensure the presence of relevant corresponding information on the website.
b) The website URL may become a part of the mail signature for all the outgoing mails from the Departments and its employees.
c) The website should also be promoted by link exchange with other Government websites as well as international websites.
d) Providing regular and updated news on various issues related to the Government, citizens etc. are very important tools of promotion. Regular revised updates on all important issues related to Government and in interest of the citizens should be highlighted/placed on the website. Frequent updates and change in contents will bring the visitors back to the portal and will keep the readers interested in the website.
e) Sending regular updates on the websites to registered and interested users through an electronic newsletter should form an important means of promotion.

12. Legal framework

Suitable legal framework for e-Commerce, secure transactions, digital signatures etc, as per the prevailing Cyber Laws of the Government of India from time to time shall be adhered to by the State Government Departments, Boards and Corporations etc. It will be the sole responsibility of the Organisation concerned to ensure adherence to the legal aspects. The Designing/Hosting Agency shall not be responsible for any legal issues arising out of the violation of any of the Cyber Laws or unauthorized use of the Web content or by way of putting up any undesirable information not permitted under law. E&IT Department shall, from time to time, apprise the Departments, Boards and Corporations etc. about the latest legal framework adopted by the Central/State Government

13. Reference links

- Registration in .GOV.IN domain : www.registry.gov.inoRegistration in .NIC.IN domain : https://webservices.nic.in/nic_in.aspxoEmpanelled Cyber Security Audit Firms : www.cert-in.org.inoGuideline for Indian Government Websites (GISW) :
  - https://guidelines.gov.in/
  - https://guidelines.gov.in/assets/gigw-manual.pdf
  - https://web.guidelines.gov.in/assets/documents/pdf/hand_book.pdf

- Open Web Application Security Project (OWASP) Guideline :
  - https://www.owasp.org
  - https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf
  - https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf
  - https://code.google.com/archive/p/owasptop10/
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
  - https://www.owasp.org/index.php/OWASP_Web_Testing_Environment_Project
- National Cyber Security Policy
  - http://meity.gov.in/writereaddata/files/ncsp_060411.pdf
  - http://164.100.94.102/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf
  - http://digitalindia.gov.in/writereaddata/files/MeitY_Cyber%20Security_13%20Feb_Final.pdf
  - https://niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

Annexure-I

(*****Fields are mandatory***)

Government OfIndia

National Information Centre

.gov.in domain name details from

For Office Use:

Domain ID: ..... (Will be generated after submitting the request)
Registration Date: .....

Desired Domain Name* WWW. [ ] .GOV.IN

Ministry/Department/Organization Contact

Name*

Designation*

Organization*

Address1*

City* **Pincode***

State/ Province* **Country*** INDIA

Telephone* **+91** Mobile

Fax **+91** **Email***

(must be in *@nic.in* or *@gov.in*)

Administrative Contact(Must be other than the Ministry/Department/OrganizationContact)

Name*

Designation*

Organization*

Address1*

City* **Pincode***

State/ Province* **Country*** INDIA

Telephone* **+91** Mobile:

Fax **+91** **Email***

(must be in *@nic.in* or *@gov.in*)

Technical Contact

Name*

Designation*

Organization*

Address1*

City* **Pincode***

State/ Province* **Country*** INDIA

Telephone* **+91** Mobile

Fax **+91** **Email***
(must be in *@nic.in* or *@gov.in*)

Nameserver Details

Primary Name Server

Host Name

IP

Secondary Name Server

Host Name

IP

Tertiary Name Server (Third)

Host Name

IP

Signature with Seal

Annexure-2

National Informatics Centre

Web Site Hosting Registration Form (for GOV.IN/ NIC.IN Domains)

(Please make sure the form is filled completely and correctly to avoid delay.)

❑ (Put ✓ mark for appropriate option)

*** The cloud hosting is **chargeable** for**PSUs and Revenue Generating Government Bodies**

1.Name of the Website	**http://**
2. Title of the Web site	Official website of
3. Name of the Ministry/ Deptt./ State Organisation	
4. GOI Directory Category	❑ Central Govt. Organisations ❑ Apex Body ❑ PSUs/ Revenue generating ❑ Event ❑ State Govt. ❑ Other Bodies
5. Hosting Platform	❑ Windows ❑ LINUX
6. Interactive Components (other than html)	❑ ASP ❑ JSP/ Servets (JDK) ❑ Other ❑ ASP.Net Version: ❑ CGI (PERL, C…) ❑ Non ❑ COM/COM+ components ❑ PHP Version:
7. Database support needed	**If yes,** ❑ Yes Name of the Database: SQL Server ❑ MySQL ❑ PGSQL ❑ No Size of Database(MB): Growth Rate of database annually: MB
8. Site is Multilingual	❑ Yes ❑ No **If yes,** Mention the languages: ❑ English ❑ Odia
9. Audio/Video Components	❑ Yes ❑ No **If yes,** Mention formats: ❑ MP3 ❑ MPEG ❑ FLV ❑ AVI ❑ WMV
10. Size of the Site: (in MB)	
11. Site developed by: (Division /Organisation)	❑ NIC ❑ Non NIC For **Non-NIC** Provide Details:
12. Contact person (from NIC)	Name: Designation: NIC Centre: State /City: Pin: Email: Phone:
13. Contact person (from user)	Name: Designation: Deptt./ Organisation: State /City: Pin: Email: Phone:
14. Site is Presently /temporarily located at	http://
15. Main /Opening File	❑ welcome.html ❑ Index.html ❑ default.ht ❑ default.ht ❑ index.php ❑ Other,
16. Announcement Date	
Charges for Cloud Hosting	Presently Ministries and Departments are given free service while the hosting is **chargeable** for**PSUs** and **Revenue Generating Government Bodies**

Date:

Signature & Seal
(Head of the Department)

Payment Details (For PSUs/ Revenue Generating Government Bodies)

Amount: Cheque No /Draft No. Date:	Bank: City: Hosting Charges for no. of years

Hosting Details **(for official use only)**

Server Name: IP Address:	Alias of: HVS /SVS /Directory
Launch Date (DD/MM/YYYY):	

Annexure-2

Authorization Letter to be submitted (On official letter head in the name of Signing Authority only)

Domain ID< *Domain Id*> Domain Name :<*domainname*>.gov.in
Category of Organization : <*Select suitable category from the list given in Table -1 in the document*>
(Refer to Guideline)

Organizational Contact (Registrant) Details

Name & Designation:	Organization:	
Address:		
City:	State:	Pin:
Telephone:	Email:	

Administrative Contact Details

Name & Designation:	Organization:	
Address:		
City:	State:	Pin:
Telephone:	Email:	

Declaration:

1. I as head of the organization acknowledge that <*exact complete name of the organization*> meets all requisites to be considered as a government organization and is controlled by the <*choose either centre or state*> government.
2. I understand and agree to comply with the following Terms & Conditions of GOV.IN domain registration: -

    a. All the contact addresses entered online and authorization letter are correct and same.
    b. The contact details would be updated as and when there is a change.
    c. Domain name will not be used for any unlawful and commercial purposes.
    d. The web content of the requested domain name will conform to IT Act of India.
    e. The domain name would be renewed by sending domain name renewal request in the prescribed format one month prior to the renewal date
    f. GOV.IN registry will not be responsible for any false documents submitted, misguidance and any unlawful activities practiced by the registrant using the domain name.
    g. GOV.IN allocation will be under the conformity of.IN Domain Name Dispute Resolution Policy (INDRP).
    h. Domain shall be cancelled in case of information furnished found to be incorrect or misleading or if the GOV.IN guideline is violated.
    i. **We are aware of the OM of the GoI, MHA, No- 14/4/2001-T dated 17th July 2007 and the website will be hosted in India only.**

Signing Authority (*Organizational Contact (Registrant) Details*)

Name:	Designation:-
Organization:	Central or State:
Ministry:	
Department:	Signature with seal:

Date:
Email:

Forwarding Letter (on the Government of India / State Government official letter head in the name of Signing Authority)

To
The GOV.IN Domain name Registrar
Gov.in Registry
Room No. 379, 3rd Floor (A4B4)
National Informatics Centre (NIC)
Department of Electronics & Information Technology, MoCIT
A-Block, CGO Complex, Lodhi Road
New Delhi - 110 003

Subject: "Regarding registration of domain name <*domainame.gov.in*>".

I am hereby forwarding the Authorization Letter for the domain <*domain name*> having the domain id <*domain id*> and also confirm that all information furnished in the Authorization Letter is correct to the best of my knowledge.

I [*Name*] [*Designation*] [*Central Government Ministry or State Government Department*] endorse that the [*Organization Name*] is a government organization and belongs to the category [***Select suitable category from list given in Table-1***)] of the guidelines vide no F.No. 13/14/2014-IGD dated 6th .April 2015. The domain name [*domainname.gov.in*] would be used for official purposes and would conform to the IT Act of India and Aadhaar Act, 2016. Domain name will not be used for any unlawful & commercial purpose and as per MHA OM, the website will be hosted in India only..

Hence, I recommend "<*domainname*>.gov.in" for [*organization name*].

Signing Authority

Name:	Designation: [*Select from options give in **Table-2***]
Ministry:	Central or State:
Department:	
Organization:	Signature With Seal:
Date:	
Email:	