POLICY GUIDELINE

FOR

WEBSITE AND PORTAL

DEVELOPMENT, HOSTING AND MAINTENANCE

Content Index

1. Objective

To formulate an integrated approach to built 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 of Websites

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. Easy and fast access to the information.

   b. Global reaches.

   c. Increase in popularity.

   d. Less rush in the offices.

   e. Increased efficiency in replying to the public queries.

   f. Cost efficiency.

   g. More attractive way to advertise itself.

   h. Increased public awareness

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) and latest Open Web Application Security Project (OWASP) Developer Guideline. 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.

   b) 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

   c) 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.

   d) The website should be IPV6 Compliant and support Dual stack i.e. both IPV4 & IPV6.

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) 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.

d) Content Administrator shall approve the contents of the Website of the Department/office and a communication will be sent to concern Web Master, 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 through webmaster.

e) 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.

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

g) 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 websites updating and maintenance

The responsibility in regard to the contents of the Website shall be that of the Head of the Organisation and he will ensure timely/periodic updating of the Website. The updating of the official websites shall be done through the Web master 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 contents in respect of their organization

6. 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.

Examples:

- o Domain Name for Government Department:
  - ▪ PR Department may have domain name "PRODISHA.GOV.IN"
- o Domain Name for Line offices under a Department:
  - ▪ Bhubaneswar Block may have domain name "BLK-BBSR.ORODISHA.GOV.IN".
- o Domain Name for Districts:
  - ▪ Khurda District may have Domain name "ODISHA-KHURDA.GOV.IN"
- o Other offices like corporations, boards, agencies etc.:
  - ▪ IDCO may have website domain name IDCO.NIC.IN or IDCO.IN

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 e-Mail 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.

7. 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 Defense, Bot Protection, Account Takeover Protection, Fraud Prevention and certified accordingly..

b) In view of this the Government websites/portals should be kept in Government IT Infrastructure establishments like State Data Centre/National Data Centre, STPI, NIC 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.

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

d) 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.

e) The direct IP based hosting should be avoided.

8. <u>Guideline for security of websites</u>

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.

a) All websites or web applications should follow National Cyber Security Policy. http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf.

b) 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.

c) 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.

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

e) 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.

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

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

9. 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

   o Online or off line registration of domain names (optional)

   o Administration of Domain details i.e. Renewal of domain name, change in name server (if required), Contact updating etc.

   o Overall management of websites.

   o 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 Web Master 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.

10. 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 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

11. 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

12. Reference links

- Registration in .GOV.IN domain : www.registry.gov.in
- Registration in .NIC.IN domain : http://nicregistry.nic.in/
- Empanelled Cyber Security Audit Firms : www.cert-in.org.in
- Guideline for Indian Government Websites (GISW) :
  - http://www.darpg.nic.in/darpgwebsite_cms/Document/file/Guidelines_for_Government_websites.pdf
- Open Web Application Security Project (OWASP) Guideline :
  - https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
  - owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf
  - https://www.owasp.org/index.php/Top_10_2013-Top_10
- National Cyber Security Policy
  - http://deity.gov.in/hindi/sites/upload_files/dithindi/files/ncsp_060411.pdf

FORM-A

Domain Registration Request Form
(* - Fields are mandatory)

Required Domain Details

Domain Name* : _____.GOV.IN/NIC.IN

Term of Registration* : _____year(s) [1-2 years]

Ministry/Department/Organization Contact

Name* :_____Designation _____

Organization* : _____

Address1* : _____

Address2 : _____

City* : _____Pincode* _____State/Province* : Odisha   Country* : India

Telephone* :+91-_____ Fax: +91-_____

Mobile : _____Email* :_____
. nic.in or .gov.in

Administrative Contact

Name* :_____Designation _____

Organization* : _____

Address1* : _____

Address2 : _____

City* : _____Pincode* _____State/Province* : Odisha   Country* : India

Telephone* :+91-_____ Fax: +91-_____

Mobile : _____Email* : _____
nic.in or .gov.in

Technical Contact

Name* :_____Designation _____

Organization* : _____

Address1* :_____

Address2 :_____

City* : _____ Pincode*

Telephone* :+91-_____   Mobile : _____

Fax: +91-_____   Email* : _____
. nic.in or .gov.in

Name Server Details

If Domain is hosted in NIC/planned to be hosted in NIC _____

Primary Name Server: Host Name : _____IP: _____

Secondary Name Server: Host Name : _____IP: ____

Date: Signature of competent
authority with Seal

FORM-B

Web Information Sheet
[To be submitted to E&IT Department.]
(* - Fields are mandatory)

General Domain Details

Department :_____   Domain Name* : _____ GOV.IN/NIC.IN

Term of registration * : _____year(s) [1-2 years]   Date of expiry of registration :_____

Ministry/Department/Organization Contact

Name* : _____Designation: _____

Address1* : _____

Address2 : _____

City* : _____Pincode* _____

Telephone* :+91-_____ Fax: +91-_____

 Mobile : _____Email* :_____
. nic.in or .gov.in

Administrative Contact

Name* :_____Designation _____

Organization* : _____

Address1* : _____

Address2 : _____

City* : _____Pincode* _____

Telephone* :+91-_____ Fax: +91-_____

Mobile : _____Email* : _____
nic.in or .gov.in

Technical Contact

Name* :_____Designation _____

Organization* : _____

Address1* :_____

Address2 :_____

City* : _____ Pincode*

Telephone* :+91-_____   Mobile :   _____

Fax: +91-_____   Email* : _____
                                        . nic.in or .gov.in

Name Server Details

   If Domain is hosted in NIC/planned to be hosted in NIC _____

Primary Name Server: Host Name : _____IP: _____

Secondary Name Server: Host Name : _____IP: ____

Web site/Application developed by

Name*:_____

Organization* :_____

Address1* :_____

Address2 :_____

City* : _____ Pincode* _____ State/Province* : Odisha
Country* : India

Telephone* :+91-_____   Mobile :   _____

Fax: +91-_____   Email* : _____

Web site /application Security Audit : _____(Yes/No)
Date of last Security Audit _____

Auditor Details

Organization*:_____

Address1* :_____

Address2*: _____

City* : _____ Pincode*

Telephone : _____Fax: +91-_____   Email* : _____

Staging URL where audited : _____

Certificate Issued date : _____ Certificate No :_____

Auditor   Name

:_____

Telephone*:+91-_____ Mobile :   _____
Fax: +91- _____ Email* : _____

Web site/Application Details

Operating System :_____Web server :_____
Interactive Component (Frontend) :_____

Database (Backend) :_____
Site Type (Static /Dynamic) :_____Content
Management(Yes/No)_____
Multilingual Support _____

Hosting Server Details :

ISP name:_____ISP Address_____
Server IP Address (Web,Application & Database)

Date:

Signature of competent authority with Seal