

Website Development Checklist

Pre-Development Phase

1. Detailed CV of the developer needs to be shared by the bidder company prior to starting the development of the website.
2. For small and medium website, AMC for the website should be 1 or 2 year from the date of acceptance / go-live.
3. Department will clearly define the milestone for making payments to the software developer.
4. Development environment to be provisioned by the Bidder/Developer.
5. DIT will have it's own State Software repository of the successful projects and will ensure there is no duplication in efforts for software development.
6. Before starting the development/coding of the website, the developers are required to complete eGovernance 0.0 certification and the 5 Day eGovernance Standards (Localization, GIGW and Accessibility) training to be mandated in all the website development RFPs. Awareness for the staging environment and the APIs used as a part of SDC such as Name/Address Databases, SMS gateway, Payment Gateway, GIS, etc shall be provided as a part of the training. The training certificate shall be valid for 3 years. Renewal of certificate shall be made available online. Training would be provided free of cost, however, travel/lodging expenses, etc. will be borne by the developer/bidder.

7. GIGW training course (3 days/5 days) including Marathi Unicode & Accessibility mandatory for all developers (at least one developer/team leader for small sites, at least two for medium sites and three for large sites). The training will be held in MahaOnline office in Mumbai/Pune/Nagpur/Aurangabad centers. Training to also include Level 0 check for Top-10 vulnerabilities as per OWASP. Training would be provided free of cost, however, travel/lodging expenses, etc. will be borne by the developer/bidder.
8. Intellectual Property Rights (IPR) of the source code will vest solely with the Government of Maharashtra. However, such a system will not be allowed to be misused by quoting same software to other districts or departments, as DIT may provide the same free of cost to other Departments.
9. Representatives of software developers working on the project must sign the Non-Disclosure Agreement (NDA) with project owner of concerned department.
10. Departments to adhere to the Advisory that has been provided to All Government Departments on 30th September 2013 for :

Hosting of Government Websites, use of Official Email IDs and other Cloud based services, connecting to NIXI & Sec. 43A compliance audits, Adoption of Technical Standards for Interoperability Framework and other standards published by GoI for various eGovernance Projects

Use of Standard Components such as Payment Gateway, SMS Gateway, Email, etc would be provided

As per SDC Rate Chart.

Development Phase

1. Website needs to be Bilingual i.e. Marathi and English. By default, the webpage should open in Marathi language.
2. Website should be developed with gov.in or maharashtra.gov.in extension.
3. Website should run independent of IP Address. i.e. IP Addresses should be not be hard coded in the source code/configuration.
4. Website should be IPv6 compliant.
5. Website should be able to open in all six ways. For example,
 - a. <https://www.maharashtra.gov.in>
 - b. <http://www.maharashtra.gov.in>
 - c. www.maharashtra.gov.in
 - d. <https://maharashtra.gov.in>
 - e. <http://maharashtra.gov.in>

- f. maharashtra.gov.in
6. Website should be running on SSL i.e. http request should automatically get redirected to https
 7. Website should be compatible to run on multi server environment for load sharing
 8. Website should be compatible for accessibility from any device, any Operating System and any browser.
 9. Platform used for Website such as OS, DB, Java, etc. software should be N-1 where N is the latest version prevailing.
 10. CAPTCHA should be present for web pages with form field such as feedback form, registration form etc.
 11. Logging to be enabled for Web Server / DB Server.
 12. Password should not be hardcoded in any website configuration files or stored in plain text.
 13. Website should be in compliance with
 - eGovernance Standards of Government of India :
 - a. Technical Standards for Interoperability Framework for e-Governance (IFEG) in India Version 1.0
 - b. MDDS- Demographic Standards
 - c. Character Encoding
 - d. Font Standard
 - e. eGov.BIDS
 - f. eGov.BIDS
 - g. eSAFE-ISF01, eSAFE Framework (and associated documents)
 - h. Guidelines for Usage of Digital Signatures in e-Governance
 - i. FMG
 - j. Policy on Open Standards for e-Governance Framework for Mobile Governance
 - e-Governance policies of Government of Maharashtra
 - Guidelines of Indian Government Website (GIGW)
 - WCAG 2.0
 - W3C
 - Other e-Governance standards of Government of India (egovstandards.gov.in)

Post-Development Phase

1. Level 0 check to be complied by the developer for GIGW compliance and address Top-10 vulnerabilities as per OWASP.
2. Security Audit of Website/Application:

Website/Application needs to be Security Audited by the Cert-In empanelled Security Auditors. The Security Audit clause should be part of the RFP, wherein the bidder will bear the cost of security certification.

3. Security Audit Certificate to be mandated along with Hash5 code. Source code along with Hash5 code of the website to be submitted by Developer. Documentation of Source Code along with Administration/User Manuals needs to be submitted.
4. DIT would also facilitate the checks for GIGW compliance and Accessibility of the website.
5. The project will be treated as "complete" only if:
 - UAT / FAT is completed
 - Handover to the Department is completed
 - Final Source code along with Security Audit Certificate (with Hash5) of the project along with detailed documentation and IPR is being transferred to DIT for State Software Repository.
6. It is advisable to host the Website in the Maharashtra State Data Centre for which below compliance needs to be adhered.
 - Details of the website such as Operating System, Database used, Web Servers used, Data Storage required, architecture, functionality, framework used etc. needs to be provided to DIT/SDC for due scrutiny.
 - After due scrutiny of the details provided to start the hosting process, developer along with department nodal officer needs to visit DIT/MH-SDC for making site available in staging area for first level security compliance check.
 - Chief Information Security Officer (CISO) of SDC will analyze the documents submitted by department along with security audit certificate, he will submit acceptance or rejection report for hosting at MH-SDC.
Department to submit hardcopy of Declaration letter, source code CD, security audit certificate etc. to Principal Secretary IT for making website/application live from production environment. Department/developer will copy the audited code to the production environment. He will install SSL certificate provided by DCO on production server. Developer will ensure port redirection from port 80 to 443.
 - Department will fill change request form (CRF) for opening port 80 & 443 for the public IP already assigned to the URL. This will be taken as standard request. All email communication will be accepted only from government email id of department nodal officer.
DCO will test URL and if it is working successfully then generates the hash code and make website/application available to public.