Guidelines for Indian Govt Websites (GIGW) 3.0

New Features and Roadmap

A. K Upadhyay, Scientist G , STQC
Lokesh Joshi, Scientist F,NIC

Ministry of Electronics and Information Technology
Government of India

Background

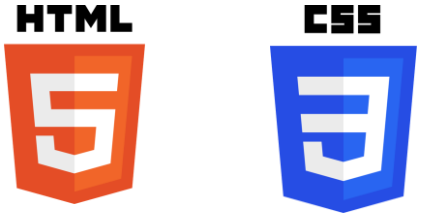
- GIGW was formulated by NIC and launched in Feb 2009
- Aims to ensure a certain common minimum benchmark for government websites in terms of Branding (government Identity) Content, Technology , Accessibility, Maintenance and Management
- GIGW deal with entire lifecycle of the website Planning Design Development Hosting Management
- Adopted by DARPG and made a part of CSMOP

GIGW ver 1

- Guidelines are divided into 3 categories
  - **Mandatory** - denoted by MUST and are directed towards requirements which the departments must necessarily comply with
  - **Advisory** - denoted by SHOULD and refer to recommended practices that are considered highly important and desirable
  - **Voluntary** - denoted by MAY and can be adopted by a department if deemed suitable
- Mandatory guidelines had to be met to ensure conformance
- STQC has formulated a website quality certification scheme based on these Guidelines

GIGW ver2 (2019)

- HTML and CSS upgrade to latest versions
- Responsive UI (Mobile compliance) was made mandatory
- New section on mobile apps included (focusing mainly on mobile app accessibility)
- Accessibility upgraded to meet all the points of WCAG 2.0 Level AA
- Compliance matrix has been made leaner and the total no of guidelines has been reduced
- Compliance matrix has been split into two sections the General Guidelines and the Accessibility Guidelines



New features in GIGW 3.0

Focus Areas

Q

QUALITY

Ensuring a user-friendly experience for visitors

25

A

ACCESSIBILITY

Creating a more inclusive digital environment (as per RPWD Act)

50

S

SECURITY

Preventing risks to website content and user data

3

L

LIFE CYCLE MANAGEMENT

Policies & Plans for website management & maintenance

10

Mapped with he risk of non conformance.

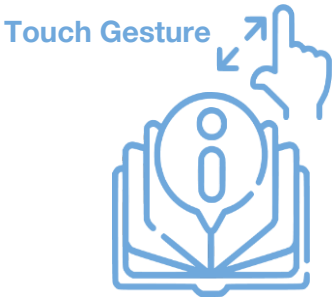
Structure

- Actionable for
  - Department
  - Developers
  - Evaluators/auditors
- Each guideline has the following attributes
  - Statement
  - Benefit
  - Actionable
    - Government department action
    - Developer action
    - Evaluator/auditor action
  - References (to external resource, if any)

Accessibility

- W3C keeps providing recommendations for improving accessibility of web content through the Web Content Accessibility Guideline (WCAG), which is adopted worldwide as the benchmark for accessibility:
- Meets WCAG 2.1 Level AA - latest set of guidelines released by W3C
- Focused on improving touch gesture accessibility, which is an important aspect of mobile device accessibility
- 17 new guidelines added and reference to corresponding WCAG guideline given

Inclusive Digital Environment



Quality and Lifecycle

- Guideline on the integration of Social media platforms for two way interaction with citizens
- Consisent UI across the websites of a department
- API integration with digital platforms
  - Digilocker
  - Aadhaar
  - India Portal
- Provides templates for policies, plans and processes:
  - Content Contribution, Moderation & Approval Policy (CMAP)
  - Content Archival Policy (CAP)
  - Content Review Policy (CRP)
  - Copyright Policy
  - Hyper-Linking Policy
  - Website Monitoring Plan
  - Terms & Conditions

Security 1/2

- A new chapter on cybersecurity, formulated by CERT-In, has also been incorporated
- Covers Web Application Security, Mobile Application Security, Infrastructure Security
- Based on the industry best security practices and guidelines such as ISO 27001, OWASP ASVS, OWASP Top 10 vulnerabilities and CIS benchmarks as per the prevailing security policy.
- Must be used in conjunction with the guidance and advisories issued by CERT-In from time to time and should be treated as updates to the guidance contained in the chapter on cybersecurity.

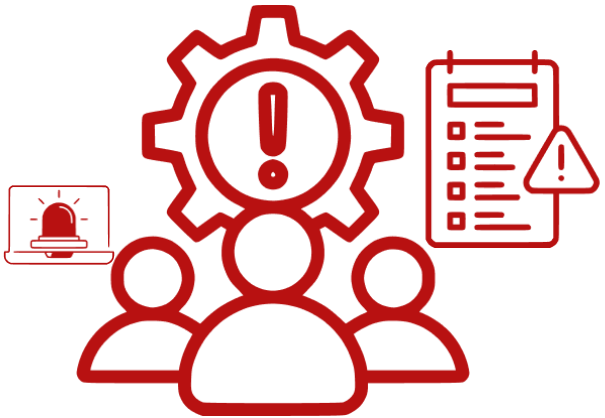
Security 2/2

- Website, web application, web portal or mobile app is Security Audited (Security Audit Clearance certificate)
  - Code Security
  - Database Security
  - OWASP Top 10
- Hosting Environment has been secured (C I A)
  - Secure web infrastructure
  - Hardened Component
- Website has the Security Policy, Privacy Policy and the Contingency Management Plan
  - Policies- Defined and documented
  - Actions being taken as per defined policies
  - Monitoring

Risk Mitigation

- GIGW 3.0 is a risk based guidelines
- Risks pertaining to poor quality, bad accessibility and weak security have been identified.
  - Poor Quality (10)
  - Bad Accessibility (9)
  - Weak Security (15)
- Requirements to counter the risks have been specified
- by following the GIGW, organisations can mitigate risks and ensure a secure and user-friendly experience for their website visitors

Risk mitigation is a crucial aspect of any standard/guideline.



Roadmap

- Go through Checklist (GIGW 3.0)
- Identify Gap areas
- Review developer's actions & Department's Actions
- Check compliance
- Prepare WQM (Template Available at STQC Website)
- Apply for Certification

Maintain conformance and periodically monitor the website

Thank you

Security GIGW 1.0

103	**7.7.1 & 7.7.2 - Website has cleared Security Audit by certified agency and has a Security Policy.**
104	8.2.1 - Websites are accessible to the intended audience in an efficient and secure manner on 24x7 basis.
105	8.2.1(a) & 8.2.1(b) - The Hosting Service Provider possesses state-of-the art multi-tier security infrastructure as well as devices such as firewall and intrusion prevention systems.
106	8.2.1(c) - The Hosting Service Provider has redundant server infrastructure for high availability.
107	8.2.1(d) - The Hosting Service Provider performs regular backup of the website.
108	8.2.1(e) - The Hosting Service Provider has a Disaster Recovery (DR) Centre in a geographically distant location and a well crafted DR plan for the website.
109	8.2.1(i) - Web Hosting Service Provider provides Helpdesk & technical support on 24x7x365 basis.
110	8.3 - All possible security measures have been taken to prevent defacement/ hacking of the website and the department has contingency plan in place for situations like these.

Security GIGW 2.0

3	**Website has the following clearly defined policies and plans approved by the web information manager.** **..** **9. Contingency Management Plan.** **10. Security Policy.**
29	Website has cleared security audit.
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

Security GIGW 3.0

1	**The website, web application, web portal or mobile app is Security Audited and an Audit Clearance certificate is issued by NIC, STQC or a CERT-In empaneled vendor before hosting in production environment.**
2	Hosting Environment must be secured for ensuring confidentiality, integrity and availability (CIA).
3	Website has clearly defined Security Policy, Privacy Policy and Contingency Management Plan approved by the Web Information Manager.