# Guidelines for Indian Govt Websites (GIGW ) 3.0

## New Features

Ministry of Electronics and Information Technology
Government of India

एनआईसी National Informatics Centre

# 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.

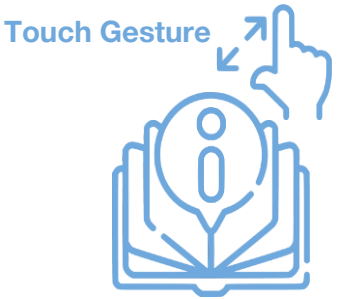
# Structure

- 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 of which 12 in level A and AA
  - 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

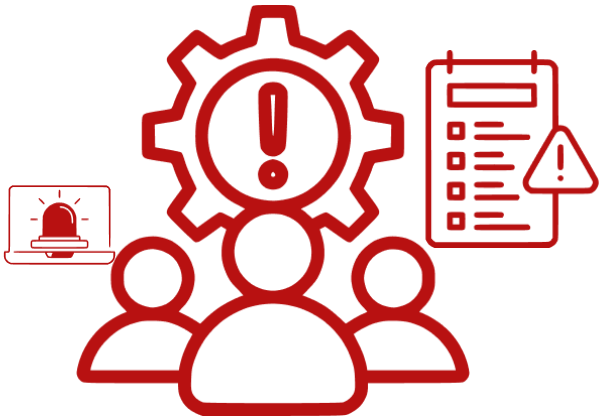
# Security

- A new chapter on cybersecurity, formulated by CERT-In,
- Covers Web Application Security, Mobile Application Security, Infrastructure Security
- Based on the industry best security practices and guidelines
- Must be used in conjunction with the guidance and advisories issued by CERT-In from time to time
- Actionables are
  - Website, web application, web portal or mobile app must be Security Audited (Security Audit Clearance certificate)
  - Hosting Environment must be secured
  - Website must have Security Policy, Privacy Policy and the Contingency Management Plan

# 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.**



# Implementation

- Go through Checklist (GIGW 3.0)
- Identify Gap areas
- Review developer's actions & Department's Actions
- Fix non compliance
- Apply for Certification

**Maintain conformance and periodically monitor the website**

# Thank you