IIT Kanpur invites bids for checking the latest GIGW conformity and Critical Application Security Vulnerabilities of the Website.

Website Security Audit is actively evaluating web pages to ensure that they have been developed within the guidelines of security best practices. It can be undertaken as part of a more exhaustive security audit or in isolation. It is of great importance to avoid security holes in the application itself. It improves the reliability, stability, and performance of the application. The application testing results are delivered in a comprehensive report highlighting the vulnerabilities and mitigating the risk.

Bidders have to share the complete compliance sheet details along with the mechanism they are going to follow for the due process.

Specific Requirements & Scope

Website Details:

S. No.	Parameters	Description
1	**Web Application Name & URL**	https://iitk.ac.in/
2	**Developer Contact Details**	Organization Name: IIT Kanpur **Contact Person Name:** Dr. Nisanth N. Nair (DDIA) Email ID: ddia@iitk.ac.in Prajwal Bajpai Email ID: prajwalb@iitk.ac.in
3	**Application hosted on**	Private Server
4	**Application Server**	Apache
5	**Front-end Tool**	PHP
6	**Back-end Database**	MySQL
7	**Operating System Details**	Linux
8	**Whether the application contains any content management**	Yes, Joomla

	module(CMS) (If yes then which?)	
9	**Authorization No. of roles & types of privileges for the different roles**	Joomla User Roles & Privileges Public – The lowest role with no special access. Registered – Can log in and access registered-only content. Author – Can submit and edit their own articles. Editor – Can edit all articles. Publisher – Can publish and manage articles. Manager – Can manage site content but has no system-level access. Administrator – Can manage most site functions except core system settings. Joomla Privileges: Content Management: Creating, editing, and publishing articles. User Management: Assigning user groups and permissions. Component Management: Access to extensions, modules, and plugins.
10	**Total No. (Approximate) of Input Forms**	2 forms (In running website iitk.ac.in)
11	**Total number of input fields**	8 fields
12	**No. of login modules**	1
13	**Is there any payment gateway?**	NO
14	**Whether the application/website was audited earlier. If yes, then mention the year also.**	NO
15	**No. of Dynamic Pages**	CMS based website.

The matrix to check conformity should be as per the latest GIGW Standards

S/N	Quality Guidelines:	Risks Addressed
1	Association with the Government is demonstrated using Emblem/Logo in proper ratio and colour, prominently displayed on the homepage/home screen of the website/app.	Q8
2	Ownership information is displayed on the homepage/ home screen and on all important entry pages/screens of the website/app, and each subsequent page/screen is a standalone entity in terms of ownership, navigation, and context of content.	Q8
3	Source of all documents, not owned by the dept. that have been reproduced in part or in full, is mentioned.	Q3
4	Due permissions have been obtained for publishing any content protected by copyright.	Q3
5	The homepage/home screen of the website displays the last updated/reviewed date	Q7
6	Complete information, including title, size, format, and usage instructions, is provided for all downloadable material.	Q7
7	Statement: With respect to each, Circular, Notification, Document, Form, Scheme, Service, and Recruitment notice, the following should be clearly listed on the Website: (a) Complete title (b) Language (if other than English) (c) Purpose/procedure to apply (as applicable) (d) Validity (if applicable)	Q7
8	All outdated Announcements, Tenders, Recruitment notices, News and Press Releases are removed from the website and/or placed into the archives as per the archival policy.	Q7
9	All information about the government organization, useful for the citizen and other stakeholders, is present in the 'About Us' section, and a mechanism is in place to keep the information up to date.	Q6, Q7

10	The website has a 'Contact Us' page providing complete contact details of important functionaries in the government organization, and this is linked from the homepage/home screen and all relevant places on the website/app.	Q6, Q7
11	Feedback is collected through online forms, and a mechanism is in place to ensure a timely response to feedback/queries received through the website.	Q10
12	The website provides a prominent link to the 'National Portal' from the homepage, and subsequent pages belonging to the National Portal load in a new browser window.	Q7
13	The website has been tested on multiple browsers. Hindi/Regional language fonts have been tested on popular browsers for any inconsistency (loss of layout).	Q9
14	The website has a readily available Help section linked from all pages of the website.	Q6, Q7
15	Website uses Cascading Style Sheets (CSS) to control layouts/styles and incorporates responsive design features to ensure that the interface displays well on different screen sizes.	Q9
16	The website is readable even when style sheets are switched off or not loaded.	Q9
17	Proper page title and language attribute, along with metadata for a page, like keywords and description, are appropriately included.	Q9
18	Minimum content as prescribed in the guidelines is present on the homepage/home screen and all subsequent pages/screens.	Q6, Q7
19	Data tables have been provided with the necessary tags/markup.	Q9
20	The content of the web page prints correctly on an A4 size paper	Q9
21	API integration with key government platforms (India Portal, DigiLocker, Aadhaar, Single-Sign-On, MyGov, Data Platform, MyScheme) and similar websites of the government organisation must be enabled for seamless exchange of Information and data.	Q7, Q8, Q10

22	The government organization must ensure a consistent user experience and visual identity across all its websites/apps.	**Q1, Q4, Q9**
23	Websites/apps must provide integration with popular social media.	**Q1, Q3, Q5, Q7**
24	Website is in the nic.in or gov.in domain. Educational Institutions and Research and Academic Institutions, which are eligible for registration under 'gov.in' may use 'edu.in', 'res.in' or 'ac.in' domains.	**Q8**
25	The language is free from spelling and grammatical errors.	**Q7, Q9**

S/N	Accessibility Guidelines:	Reference	Risks Addressed
1	All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below.	WCAG 2.1 – 1.1.1	A1
2	For pre-recorded audio-only and pre-recorded video-only media, the following are true, except when the audio or video is a media alternative for text and is clearly labelled as such: (a) Pre-recorded Audio-only: An alternative for time-based media is provided that presents equivalent information for pre-recorded audio-only content. (b) Pre-recorded Video-only: Either an alternative for time-based media or an audio track is provided that presents equivalent information for pre-recorded video-only content.	WCAG 2.1 – 1.2.1	A1
3	Captions are provided for all pre-recorded audio content in synchronised media, except when the media is a media alternative for text and is clearly labelled as such.	WCAG 2.1 – 1.2.2	A1
4	An alternative for time-based media or audio description of the pre-recorded video content is provided for synchronised media, except when the media is a media alternative for text and is clearly labelled as such.	WCAG 2.1 – 1.2.3	A1
5	Captions are provided for all live audio content in synchronized media.	WCAG 2.1 – 1.2.4	A1
6	Audio description is provided for all pre-recorded video content in synchronized media.	WCAG 2.1 – 1.2.5	A1
7	Information, structure and relationships conveyed through presentation can be programmatically determined or are available in text.	WCAG 2.1 – 1.3.1	A6, A9

8	When the sequence in which content is presented affects its meaning, a correct reading sequence can be programmatically determined.	WCAG 2.1 - 1.3.2	A6, A9
9	Instructions provided for understanding and operating content do not rely solely on sensory characteristics of components such as shape, colour, size, visual location, orientation, or sound.	WCAG 2.1 - 1.3.3	A1, A2, A3, A4
10	Content does not restrict its view and operation to a single display orientation, such as portrait or landscape, unless a specific display orientation is essential.	WCAG 2.1 -1.3.4	A4, A5
11	The purpose of each input field collecting information about the user can be programmatically determined when: (a) The input field serves a purpose identified in the Input Purposes for User Interface Components section; and (b) The content is implemented using technologies with support for identifying the expected meaning for form input data.	WCAG 2.1-1.3.5	A6
12	Colour is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	WCAG 2.1 - 1.4.1	A1
13	If any audio on a Web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level.	WCAG 2.1 - 1.4.2	A4, A5

14	The visual presentation of text and images of text has a contrast ratio of at least 4.5:1, except for the following: (a) Large Text: (18 pt. or 14 pt. bold) Large-scale text and images of large-scale text have a contrast ratio of at least 3:1. (b) Incidental: Text or images of text that are part of an inactive user interface component, that are pure decoration, that are not visible to anyone, or that are part of a picture that contains significant other visual content, have no contrast requirement. (c) Logotypes: Text that is part of a logo or brand name has no contrast requirement.	WCAG 2.1 - 1.4.3	A1
15	Except for captions and images of text, text can be resized without assistive technology up to 200 percent without loss of content or functionality.	WCAG 2.1 - 1.4.4	A1, A4
16	If the technologies being used can achieve the visual presentation, text is used to convey information rather than images of text, except for the following: (a) Customizable: The image of text can be visually customized to the user's requirements. (b) Essential: A particular presentation of text is essential to the information being conveyed.	WCAG 2 1 - 1.4.5	A1
17	(a) Content can be presented without loss of information or functionality and without requiring scrolling in two dimensions for: (b) Vertical scrolling content at a width equivalent to 320 CSS pixels. (c) Horizontal scrolling content at a height equivalent to 256 CSS pixels. (d) Except for parts of the content which require a two-dimensional layout for usage or meaning.	WCAG 2.1-1.4.10	A6

18	The visual presentation of the following has a contrast ratio of at least 3:1 against adjacent colour(s): (a) User Interface Components: Visual information required to identify user interface components and states, except for inactive components or where the appearance of the component is determined by the user agent and not modified by the author. (b) Graphical Objects: Parts of graphics required to understand the content, except when a particular presentation of graphics is essential to the information being conveyed.	WCAG 2.1- 1.4.11	A6
19	In content implemented using markup languages that support the following text style properties, no loss of content or functionality occurs by setting all of the following and by changing no other style property: (a) Line height (line spacing) to at least 1.5 times the font size. (b) Spacing following paragraphs to at least 2 times the font size. (c) Letter spacing (tracking) to at least 0.12 times the font size. (d) Word spacing to at least 0.16 times the font size. (e) Exception: Human languages and scripts that do not make use of one or more of these text style properties in written text can conform using only the properties that exist for that combination of language and script.	WCAG 2.1- 1.4.12	A6

20	Where receiving and then removing pointer hover or keyboard focus triggers additional content to become visible and then hidden, the following are true: (a) Dismissible: A mechanism is available to dismiss the additional content without moving pointer hover or keyboard focus unless the additional content communicates an input error or does not obscure or replace other content. (b) Hover-able: If pointer hover can trigger the additional content, then the pointer can be moved over the additional content without the additional content disappearing. (c) Persistent: The additional content remains visible until the hover or focus trigger is removed, the user dismisses it, or its information is no longer valid.	WCAG 2.1-1.4.13	A4, A5, A6
21	All functionality of the content is operable through a keyboard interface without requiring specific timings for individual keystrokes, except where the underlying function requires input that depends on the path of the user's movement and not just the endpoints.	WCAG 2.1 – 2.1.1	A5
22	If keyboard focus can be moved to a component of the page using a keyboard interface, then focus can be moved away from that component using only a keyboard interface and, if it requires more than unmodified arrow or tab keys or other standard exit methods, the user is advised of the method for moving focus away.	WCAG 2.1 – 2.1.2	A5
23	If a keyboard shortcut is implemented in content using only letter (including upper- and lower-case letters), punctuation, number, or symbol characters, then at least one of the following is true: (a) Turn off: A mechanism is available to turn the shortcut off. (b) Remap: A mechanism is available to remap the shortcut to include one or more non-printable keyboard keys (e.g., Ctrl, Alt). (c) Active only on focus: The keyboard shortcut for a user interface component is only	WCAG 2.1 – 2.1.4	A5

	active when that component has focus.		
24	For each time limit that is set by the content, at least one of the following is true: (a) Turn off: The user is allowed to turn off the time limit before encountering it; or Adjust: The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or (b) Extend: The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the spacebar") and the user is allowed to extend the time limit at least ten times; or (c) Real-time Exception: The time limit is a required part of a real-time event (for example, an auction), and no alternative to the time limit is possible; or (d) Essential Exception: The time limit is essential and extending it would invalidate the activity; or (e) 20-Hour Exception: The time limit is longer than 20 hours.	WCAG 2.1 - 2.2.1	A4
25	For moving, blinking, scrolling, or auto-updating information, all of the following are true: (a) Moving, blinking, scrolling: For any moving, blinking or scrolling information that (1) starts automatically, (2) lasts more than five seconds and (3) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it unless the movement, blinking, or scrolling is part of an activity where it is essential; and (b) Auto-updating: For any auto-updating information that (1) starts automatically and (2) is presented in parallel with other content, there is a mechanism for the user to pause, stop, or hide it or to control the frequency of the update unless the auto-updating is part of an activity where it is essential.	WCAG 2.1 - 2.2.2	A2, A4
26	Web pages do not contain anything that flashes more than three times in any one second period, or the flash is below the general flash and red flash thresholds.	WCAG 2.1 - 2.3.1	A2

27	A mechanism is available to bypass blocks of content that are repeated on multiple Web pages.	WCAG 2.1 - 2.4.1	A6
28	Web pages have titles that describe the topic or purpose.	WCAG 2.1 - 2.4.2	A6
29	If a Web page can be navigated sequentially and the navigation sequences affect meaning or operation, focusable components receive focus in an order that preserves meaning and operability.	WCAG 2.1 - 2.4.3	A6
30	The purpose of each link can be determined from the link text alone or from the link text together with its programmatically determined link context, except where the purpose of the link would be ambiguous to users in general.	WCAG 2.1 - 2.4.4	A6
31	More than one way is available to locate a Web page within a set of Web pages except where the Web Page is the result of, or a step in, a process.	WCAG 2.1 - 2.4.5	A6
32	Headings and labels describe topic or purpose.	WCAG 2.1 - 2.4.6	A6, A9
33	Any keyboard-operable user interface has a mode of operation where the keyboard focus indicator is visible.	WCAG 2.1 - 2.4.7	A4
34	All functionality that uses multipoint or path-based gestures for operation can be operated with a single pointer without a path-based gesture, unless a multipoint or path-based gesture is essential.	WCAG 2.1-2.5.1	A4
35	For functionality that can be operated using a single pointer, at least one of the following is true: (a) No Down-Event: The down-event of the pointer is not used to execute any part of the function. (b) Abort or Undo: Completion of the function is on the up-event and a mechanism is available to abort the function before completion or to undo the function after completion. (c) Up Reversal: The up-event reverses any	WCAG 2.1- 2.5.2	A4

	outcome of the preceding down-event. (d) Essential: Completing the function on the down-event is essential.		
36	For user interface components with labels that include text or images of text, the name contains the text that is presented visually.	WCAG 2.1- 2.5.3	A9
37	Functionality that can be operated by device motion or user motion can also be operated by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: (a) Supported Interface: The motion is used to operate functionality through an accessibility supported interface. (b) Essential: The motion is essential for the function and doing so would invalidate the activity. (c) Functionality that can be operated by device motion or user motion must also be operable by user interface components and responding to the motion can be disabled to prevent accidental actuation, except when: (d) Supported Interface: The motion is used to operate functionality through an accessibility supported interface. (e) Essential: The motion is essential for the function and doing so would invalidate the activity.	WCAG 2.1- 2.5.4	A5
38	The default human language of each Web page can be programmatically determined.	WCAG 2.1 - 3.1.1	A1, A6, A7
39	The human language of each passage or phrase in the content can be programmatically determined except for proper names, technical terms, words of indeterminate language and words or phrases that have become part of the vernacular of the immediately surrounding text.	WCAG 2.1 - 3.1.2	A1, A6, A7
40	When any user interface component receives focus, it does not initiate a change of context.	WCAG 2.1 - 3.2.1	A6

41	Changing the setting of any user interface component does not automatically cause a change of context unless the user has been advised of the behavior before using the component.	WCAG 2.1 - 3.2.2	A6
42	Navigational mechanisms that are repeated on multiple Web pages within a set of Web pages occur in the same relative order each time they are repeated, unless a change is initiated by the user.	WCAG 2.1 - 3.2.3	A6
43	Components that have the same functionality within a set of Web pages are identified consistently.	WCAG 2.1 - 3.2.4	A6
44	If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.	WCAG 2.1 - 3.3.1	A6
45	Labels or instructions are provided when content requires user input.	WCAG 2.1 - 3.3.2	A9
46	If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content.	WCAG 2.1 - 3.3.3	A4, A6
47	For Web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true: (a) Reversible: Submissions are reversible. (b) Checked: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them. (c) Confirmed: A mechanism is available for reviewing, confirming and correcting information before finalising the submission.	WCAG 2.1 - 3.3.4	A8

48	In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes and any IDs are unique, except where the specifications allow these features.	WCAG 2.1 - 4.1.1	A6
49	For all user interface components (including but not limited to form elements, links and components generated by scripts), the name and role can be programmatically determined; states, properties and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.	WCAG 2.1 - 4.1.2	A6
50	In content implemented using markup languages, status messages can be programmatically determined through role or properties such that they can be presented to the user by assistive technologies without receiving focus.	WCAG 2.1– 4.1.3	A6

S/N	Security Guidelines	Risks Addressed
1	Ensure that 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.	S1- S15
2	Hosting Environment must be secured to ensure confidentiality, integrity and availability (CIA).	S1- S15
3	Website has the Security Policy, Privacy Policy and the Contingency Management Plan clearly defined policies and plans approved by the government organisation.	S1- S15

S/N	Lifecycle Management Guidelines	Risks Addressed
1	The government organization has nominated a WIM as defined in the guidelines.	Q1
2	It has been ensured that all stationery of the government organization as well as advertisements/public messages issued by the government organization concerned prominently display the URL of the web site.	Q2
3	The website has the following clearly defined policies and plans approved by the WIM. (a) Copyright Policy (b) Content Contribution, Moderation and Approval (CMAP) policy (c) Content Archival (CAP) policy (d) Content Review (CRP) policy (e) Hyperlinking Policy (f) Privacy Policy (g) Terms & Conditions (h) Website Monitoring Plan. (i) Contingency Management Plan (j) Security Policy	Q3, Q4, Q5, Q7
4	The mechanism is in place to check the accuracy of Hyperlinked Content, and clear indications are given when a link leads to a non-government website.	Q4
5	It is ensured through content moderation and approval policy that Website content is free from offensive/discriminatory language.	Q7
6	Documents/Pages in multiple languages are updated simultaneously.	Q7
7	Mechanism is in place to ensure that there are no 'broken links' (internal as well as external) or 'Page not found' errors.	Q7
8	There are no links to 'under construction' pages.	Q7
9	Documents are provided either in HTML or other accessible formats.	Q9
10	The website is bilingual with a prominent language selection link and uses Unicode characters.	Q9, Q6, Q7