Website Security Policy

1. Website Monitoring Policy

Website is monitored periodically to address and fix the quality and compatibility issues around the following parameters:

Performance: Site download time is optimized for a variety of network connections as well as devices. All-important pages of the website are tested for this.

Functionality: All modules of the website are tested for their functionality. The interactive components of the site such as, feedback forms are working smoothly.

Broken Links: The website is thoroughly reviewed to rule out the presence of any broken links or errors.

Traffic Analysis: The site traffic is regularly monitored to analyse the usage patterns as well as visitors' profile and preferences.

Feedback: Feedback from the visitors is the best way to judge a website's performance and make necessary improvements. A proper mechanism for feedback is in place to carry out the changes and enhancements as suggested by the visitors.

2. Content Archival Policy:

The content components are created with metadata, source and validity date. There would be some content which is permanent in nature and for such content it is assumed that the content would reviewed in every ten years unless it is edited / deleted based on requirement. The content shall not be displayed on the Website after the validity date.

Some of the short lived content components like tenders, recruitment etc., which will not have any relevance on the website after the intended purpose.

The content components like documents, reports, latest news is regularly reviewed as per the Content Review Policy.

The content is reviewed at least two weeks prior to the validity date and if required content will be revalidated and validity date is modified. If content is not relevant, then the content is archived and no longer published on the Website.

3. Content Contribution, Moderation And Approval Policy

Content would be contributed by the authorized Content Manager in a consistent fashion to maintain uniformity and to bring in standardization along with associated metadata and keywords. In order to present the content as per the requirement of the viewer, organize the content in categorized manner and to retrieve the relevant content efficiently, the content is

contributed to the website through a Content Management System which would be web-based having user-friendly interface.

The content on the website goes through the entire life-cycle process of:-

- Creation
- Modification
- Approval
- Moderation
- Publishing
- Expiry

Once the content is contributed it is approved and moderated prior to being published on the Website. If the content is rejected at any level then it is reverted back to the originator of the content for modification.

4. Content Review Policy

All possible efforts need to be taken to keep the content on the Website current and up-to-date. This Content Review Policy defines the roles and responsibilities of the website content review and the manner in which it need to be carried out. Review Policies are defined for the diverse content elements.

The Review Policy is based on different type of content elements, its validity and relevance as well as the archival policy.

The entire website content would be reviewed for syntax checks once a month by the "HSL" Team.

5. Website Security Policy

"HSL" website contains information which is freely accessible, and may be viewed by any visitor. However, the website maintains a copyright interest in the contents of all of its websites.

Except for authorized security investigations and data collection, no attempts will be made to identify individual users. Accumulated data logs will be scheduled for regular deletion. The Website Privacy Policy details our position regarding the use of personal information provided by customers/visitors.

Unauthorized attempts to upload information or change information are strictly prohibited, and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act.

User ID and Password Policy:

Access to sensitive or proprietary business information on “HSL” website is limited to users who have been determined to have an appropriate official reason for having access to such data. All registered users who are granted security access will be identified by a user name provided by web information manager.

Users who are granted password access to restricted information are prohibited from sharing those passwords with or divulging those passwords to any third parties. User will notify us immediately in the event a User ID or password is lost or stolen or if User believes that a non-authorized individual has discovered the User ID or password.

6. Disclaimer

The official website of HSL is designed and developed by NICSI in compliance with GIGW. This website is hosted by "NIC", Hyderabad.

Though all efforts have been made to ensure the accuracy and currency of the content on this website, the same should not be construed as a statement of law or used for any legal purposes. In case of any ambiguity or doubts, users are advised to verify/check with the Department, and to obtain appropriate professional advice.

Under no circumstances will HSL be liable for any expense, loss or damage including, without limitation, indirect or consequential loss or damage, or any expense, loss or damage whatsoever arising from use, or loss of use, of data, arising out of or in connection with the use of this website.

These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the jurisdiction of the courts of India.

The information posted on this website could include hypertext links or pointers to information created and maintained by organisation. "HSL" is providing these links and pointers solely for your information and convenience. When you select a link to an outside website, you are leaving the "HSL" website and are subject to the privacy and security policies of the owners/sponsors of the outside website.

7. Website Contingency Management Policy

The presence of the website on the Internet and very importantly the site is fully functional all the times. It is expected of the Government websites to deliver information and services on round

the clock basis. Hence, all efforts should be made to minimize the downtime of the website as far as possible.

It is therefore necessary that a proper Contingency Plan to be prepared in handle any eventualities and restore the site in the shortest possible time. The possible contingencies include:

Defacement of the website: All possible security measures must be taken for the website to prevent any possible defacement/hacking by unscrupulous elements. However, if despite the security measures in place, such an eventuality occurs, there must be a proper contingency plan, which should immediately come into force. If it has been established beyond doubt that the website has been defaced, the site must be immediately blocked. The contingency plan must clearly indicate as to who is the person authorised to decide on the further course of action in such eventualities. The complete contact details of this authorised person must be available at all times with the web management team. Efforts should be made to restore the original site in the shortest possible time. At the same time, regular security reviews and checks should be conducted in order to plug any loopholes in the security.

Data Corruption: A proper mechanism has to be worked out by the concerned in consultation with their web hosting service provider to ensure that appropriate and regular back-ups of the website data are being taken. These enable a fast recovery and uninterrupted availability of the information to the citizens in view of any data corruption.

Hardware/Software Crash: Though such an occurrence is a rarely, still in case the server on which the website is being hosted crashes due to some unforeseen reason, the web hosting service provider must have enough redundant infrastructure available to restore the website at the earliest.

Natural Disasters: There could be circumstances whereby due to some natural calamity, the entire data center where the website is being hosted gets destroyed or ceases to exist. A well planned contingency mechanism has to be in place for such eventualities whereby should be ensured that the Hosting Service Provider has a 'Disaster Recover Centre (DRC)' set up at a geographically remote location and the website is switched over to the DRC with minimum delay and restored on the Net.

Apart from the above, in the event of any National Crisis or unforeseen calamity, Government websites are looked upon as a reliable and fast source of information to the public. A well-defined contingency plan for all such eventualities must be in place so that the emergency information/contact help-lines could be displayed on the website without any delay. For this, the concerned person in the HSL responsible for publishing such emergency information must be identified and the complete contact details should be available at all times.