SECRET

Pl issue an appropriate advisory to all secretaries of HOD's and endorse copy to State Director NIC
Addl CS (Home)
Pr Secy (IT).
23/4/2020

Nachiketa Jha
Deputy Director

DO. No. 501 (3)/P-III/2020- 467

आसूचना ब्यूरो
गृह मन्त्रालय
भारत सरकार
Intelligence Bureau
Ministry of Home Affairs
Government of India

Shimla, dated, the April 22, 2020

Dear Sir,

Kindly refer to our earlier communication, issued from file of even number dated April 14, 2020, regarding the advisory against use of video conferencing using Zoom application and request to use NIC Video Conferencing Application instead.

2. In the current situation, many Ministries and Government Departments are extensively using Video Conferencing (VC) apps for day to day functioning. Similarly, email is being relied upon more by officers for official communication from both, office as well as residence. With the rising number of COVID-19 related phishing attempts, it is imperative that Ministries and Government Departments use only trusted and secure VC applications and email services.

23.4.20
JS (H)

3. It is, therefore suggested that:

- For all Government to Government VC requirements and email communications, users may be advised to use VC facility and email services of NIC only for unclassified communication. (The details regarding VC usage, registration, procedure, etc. are available at vidcon.nic.in). User manual attached as Annexure-I.

- In the case of Government to non-Government VC requirement, such VCs should be secured with:

  - Setting random new user ID and strong password for each meeting,
  - Restricting/disabling file transfer option,
  - Allowing only permitted user to record video conference,

- Turning off microphone and camera when not in use, and
- Not sharing the link of the meeting publicly.

4. Best practices for secure use of Video Conferencing are enclosed at Annexure-II. Further, since email is one of the attack vectors for phishing leading to compromise of systems, conventional cyber security norms and best practices for protecting the systems, as at Annexure-III, may be followed.

With warm regards,

Yours sincerely,

N. Jha 22/4/2020

(Nachiketa Jha)

Shri Anil Kumar Khachi, IAS
Chief Secretary,
Government of Himachal Pradesh,
Shimla

Copy along with enclosures to:

1. **Shri S.R. Mardi, IPS**
Director General of Police,
Government of Himachal Pradesh,
Police Hqrs.,
Shimla

2. **Shri R.D. Dhiman, IAS**
Additional Chief Secretary (Health),
Government of Himachal Pradesh,
Shimla

3. **Shri Manoj Kumar, IAS**
Additional Chief Secretary (Home),
Government of Himachal Pradesh,
Shimla

(Nachiketa Jha)

Annexure-I

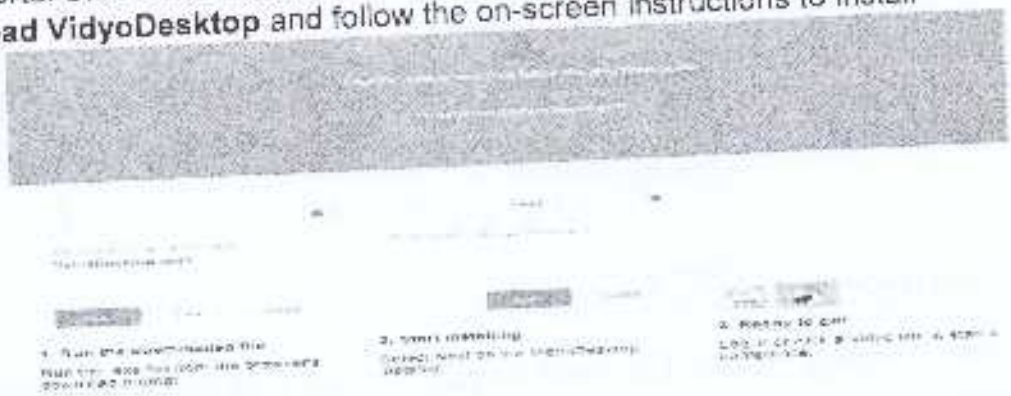
Quick user guide for use of NIC Desktop Videoconferencing for registered users

1. Prerequisite for Joining software VC based meeting

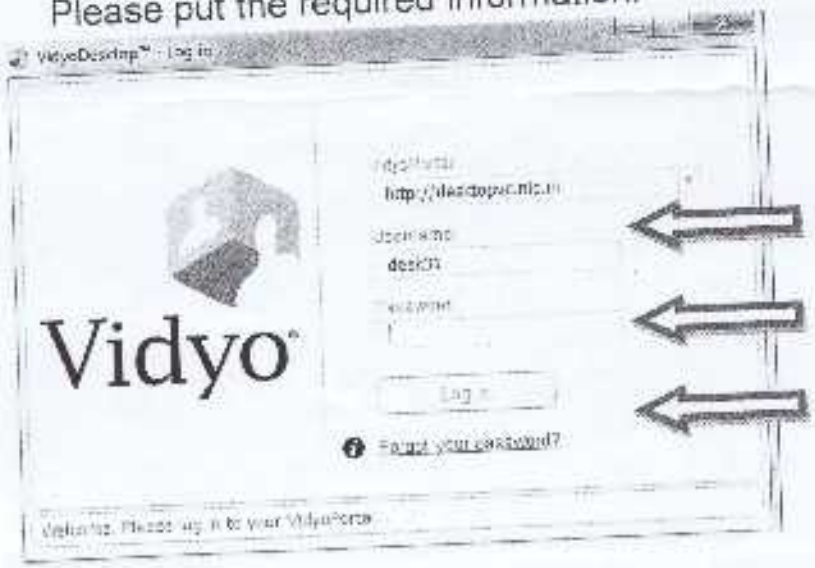
- Internet connection of 2 Mbps from any service provider (Broadband/FTTH/4G etc)
- Laptop/ Desktop working in Windows (recommended) or if wish to join form Android Phone (first download VidyoMobile from app Store and install)
- Wired Earphone/Headphones with Microphone (Strongly recommended)

2. Download Vidyo Software

Enter Portal URL either https://desktopvc.nic.in where your account is created. Click **Download VidyoDesktop** and follow the on-screen instructions to install



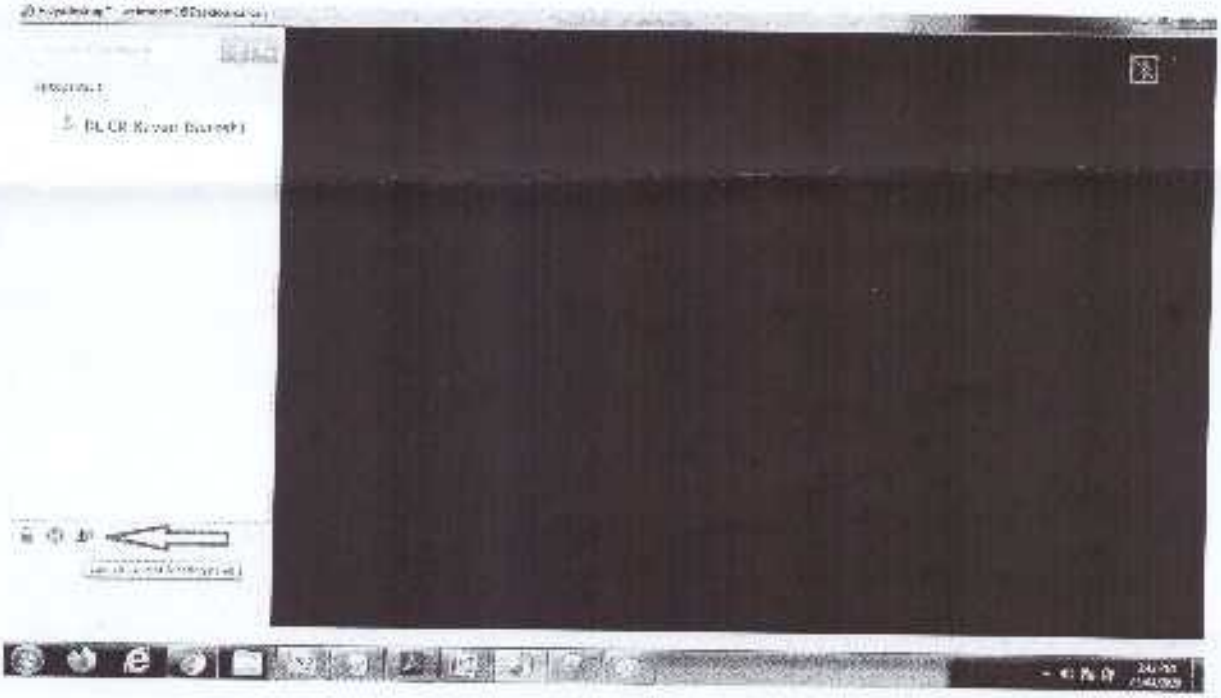
3. After Installation of vidyo desktop Application following screen will appear. Please put the required information.



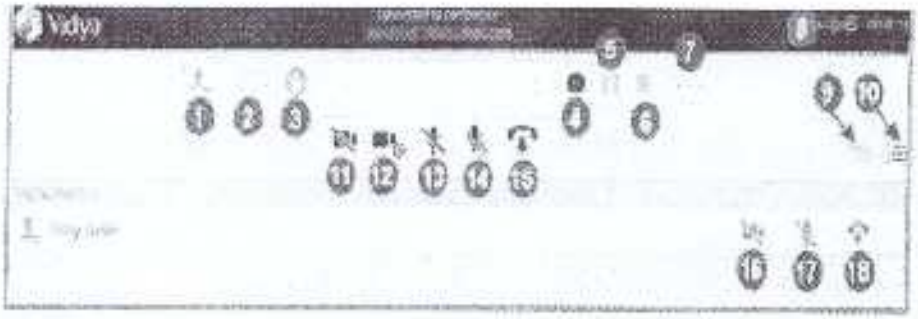
4. After putting the credentials you will get your screen like below: you will get the Webrooms Information, that you can manage by clicking

5. Select the Required Webroom which you want to control and it will show a new small window and then click on this connect to your Room option

6. After Clicking on this Connect to your Room Option you will join in to that Webroom



7. To Manage the Conference Click on Control Meeting Icon
   After Clicking this Launch Control Meeting Panel Icon you will get new window in browser



1. Click to add a participant to your room.

2. Click to invite a participant to your room via email.

3. Click to toggle between locking and unlocking your room.

4. Click to record or to record and webcast a meeting using a selected VidyoReplay™ record profile.

   This option is available only if your system includes VidyoReplay. If you need more information about which record profile to select, contact your system administrator.

5. Click to pause a recording or webcast.

   This option is available only if your system includes VidyoReplay.

6. Click to stop a recording or webcast.

   This option is available only if your system includes VidyoReplay.

7. Click to access the *Options* pop-up.

   The *Options* pop-up enables you to:

   - Access the VidyoReplay library (for systems that include VidyoReplay). For more information about the VidyoReplay library, refer to the *VidyoReplay Administrator Guide*.
   - Set a moderator PIN.
   - Set a room or webcast PIN, and create or remove a room or webcast link.

- Enable or disable Presenter Mode

  When a meeting is in Presenter Mode, the participants can view only the presenter, the audio for all the participants (except for the presenter) is muted, the participants must click the  icon on the task bar to request to speak, and the presenter can enable specific participants to speak. For more information, see Presenter Mode.

8. Click  to toggle between viewing the current meeting duration and viewing the current time of day.

9. Click to sort the list of your participants alphabetically.

10. Click  to sort the list of your participants in attendance order.

    The meeting timer is the default.

11. Click  to disable video on all participants' cameras without allowing them to re-enable it.

12. Click  to disable video on all participants' cameras while allowing them to re-enable it.

13. Click  to mute audio on all participants' microphones without allowing them to re-enable it.

14. Click  to mute audio on all participants' microphones while allowing them to re-enable it.

15. Click  to disconnect all participants from your meeting room.

16. Click  to disable video on the selected participant's camera without allowing that participant to re-enable it.

17. Click  to mute audio on the selected participant's microphone without allowing that participant to re-enable it.

18. Click  to disconnect the selected participant from your meeting room.

8. **For other Government Users accounts are being created on demand basis and user name default password will be communicated in https://desktovc.nic.in**

***

Annexure-II

Best practices for secure use of Video Conferencing (VC)

Any meeting platform if not configured properly may be vulnerable to data leakage, unauthorized access and remote take over by malicious actors. Therefore, certain common security configurations must be done in all the meeting platforms to:

- prevent unauthorised entry in the conference room;
- prevent an authorised participant to carry out malicious activities on the terminals of others in the conference;
- avoid Denial of service (DOS) attack by restricting users through passwords and access grant; and
- prevent data leakage.

2. Following configuration wherever available should be done on VC apps /services:

- Setting random new user ID and password for each meeting
- Password should be strong if set by users
- Enabling *waiting Room*, so that every user can enter only when host conducting meeting admits him
- Disabling *join before host*
- Restricting/Allowing *Screen Sharing* by host Only
- Restricting *"removed participants to re-join"*
- Restricting/disabling *file transfer* option (if not required)
- *Locking meeting*, once all attendees have joined
- Restricting the recording feature
- To end meeting (and not just leave, if you are administrator)
- Sign out of meeting account if not in use.
- Users must get permission to record a video conference from everyone on the call.
- Sensitive information should be discussed in designated video conference rooms and not in public places or open office spaces.
- Cameras and microphones should be turned off when not in use.
- Video meeting link not to be shared publicly.

******

Annexure-III

Conventional Cyber Security Norms and Best Practices

A) *Do's and Don'ts to minimize Malware infections while using Internet-connected or standalone Computers.*

Do's

1. Always use genuine software.
2. Install the latest updates/patches for Operating System, Antivirus and Application software.
3. Enable a firewall. Operating Systems have an inbuilt firewall which can be used to stop unwanted Internet connections.
4. Limit user privileges on the computer. Always access Internet as a standard user but not as Administrator.
5. Check and verify email sender IDs and web links before opening file attachments and clicking on links in emails and web pages.
6. Protect against social engineering attacks. Phishing emails and SMS are used to get user credentials like username, passwords, credit card and PIN numbers etc.
7. Regularly check the last log-in details of email accounts.
8. Use strong passwords that include a combination of letters, numbers, and symbols.
9. Use only officially supplied USB storage media. USB storage media should be regularly formatted after use to erase any malicious files hidden from normal view.
10. Regularly take backup of document files to avoid lose of files in case of emergencies like malware infections, hard disk crash, corrupted applications and other unforeseen incidents.

Don'ts

1. Avoid downloading and installing pirated software.
2. Internet-connected computers should not be used for drafting / storing sensitive official documents / correspondences.
3. Don't open emails from unknown email IDs. Such mails should be deleted from email account inbox.
4. Don't download and open file attachments that originated from unknown sources.
5. Auto storage of user name and password in browser /web page should be disabled in shared computers used for Internet activities.
6. Avoid using personal USB storage devices / Smart Devices on office computers.
7. Don't share passwords with anyone. Don't use the same password on all websites and services.

Protection tips to prevent malware infections in Windows computer.

1. Always set automatic updates for Operating System, Anti-Virus and Applications. For Windows OS auto update can be done as follows:-

   Control Panel -> Windows Updates ->Change Settings -> Install updates automatically.

   (For other software follow the steps as given in the respective software.)

2. Checking for unusual network traffic with Windows "netstat -na" command.

   Type "cmd" in "run" and type "netstat –na". Checkout foreign Established connection and IP addresses. Check the IP address for its ownership

3. Check for any unusual executable running automatically at Windows startup.

   Type "msconfig" in "run" and check for any unusual executable running automatically.

   (Disable, delete or uninstall any unnecessary /unknown executable/ program.)

4. Enable hidden files, folders and system files view to find any unusual or hidden files, especially useful while using USB storage devises.

   Control Panel -> Folder Options -> View -> select the "Show hidden files and folders" option and unselect "Hide protected operating system files"

   Make sure there is no hidden file and folders present in the USB Storage device. Format the device if any unusual files (files having extensions exe, com, dat, scr and ini etc) are present besides the data files (doc, ppt, xls and pdf etc).

5. Delete the contents of Windows "Temp" and "Temporary Internet files" regularly.

   (a) **Type %temp% in "run" and delete all the contents of temporary folder.**

   (b) **For deleting Temporary Internet Files follow steps as given by different browsers like Windows Internet Explorer / Edge, Google Chrome, Mozilla Firefox, Opera and Apple Safari.**

******