S E C T I O N P I L - W

I N T H E S U P R E M E C O U R T O F I N D I A

(ORIGINAL/CRIMINAL/CIVIL/APPELLATE JURISDICTION)

WRIT PETITION (CIVIL) NO. 1016 of 2019

IN THE MATTER OF:-

KN Govindacharya …Petitioner(s)

VERSUS

Secretary General & Ors. …Respondent(s)

INDEX

SR. NO.	PARTICULARS	COPIES	PAGE NO.	COURT FEE
1.	Interim Application seeking Directions with Affidavit	1	1-7	
2.	Annexures 1 to 6.	1	8-46	
3.				
4.				
5.				
6.				
7.				
8.				
9.				
			TOTAL	

Certified that the copies are correct.

Filed on: 18.04.2020 Filed by

Sachin Mittal
Advocate-on-Record
Supreme Court of India
AOR Code No.: 2290
3, Abul Fazal Road, LGF,
Bengali Market,
New Delhi – 110001
(Advocate for the Petitioner)
Mobile: +91-9999621615

IN THE SUPREME COURT OF INDIA

[CIVIL ORIGINAL JURISDICTION]

WRIT PETITION (C) NO. 1016/2019

PUBLIC INTEREST LITIGATION

IN THE MATTER OF:-

K.N. GOVINDACHARYA …PETITIONER

VERSUS

SECRETARY GENERAL & ORS. …RESPONDENTS

INTERIM APPLICATION FOR DIRECTIONS

PAPER BOOK

(FOR INDEX KINDLY SEE INSIDE)

ADVOCATE FOR PETITIONER: SACHIN MITTAL

INDEX

IN THE SUPREME COURT OF INDIA

[CIVIL ORIGINAL JURISDICTION]

I.A. NO. OF 2020

IN

WRIT PETITION (C) NO. 1016/2019

PUBLIC INTEREST LITIGATION

IN THE MATTER OF:-

K.N. GOVINDACHARYA …APPLICANT

VERSUS

SECRETARY GENERAL & ORS. …RESPONDENTS

INTERIM APPLICATION SEEKING DIRECTIONS

To,

THE HON'BLE CHIEF JUSTICE OF INDIA AND HIS COMPANION JUDGES OF THIS HON'BLE COURT

MOST RESPECTFULLY SHOWETH:

1. That the Petitioner has filed Writ Petition (Civil) 1016/2019, which is pending before this Hon'ble Court. In the present application, the Petitioner is seeking NIC based infrastructure/NIC audited infrastructure for communication and video conferencing for Judiciary and all government officials as well as requisite amendment in the Supreme Court

Rules, 2013 and Rules of the High Courts with necessary safeguards for hearing through video conferencing.

2. That the Hon'ble Prime Minister announced the three weeks lockdown on 24 March 2020. After the first phase of the lockdown got over, the second phase was ordered to be continued up to 03 May 2020. After the announcement of first phase, Government announced its Work from Home Policy for government servants. The notification regarding work from home was issued by the Ministry of Electronics and Information Technology on 24.03.2020 itself. The notification, which is applicable to government employees, allows WhatsApp as a method of video calling.

   True Copy of Notification vide. F.No. 17(4)/2020-Pers.I (Pt) dated 24.03.2020 for Work From Home issued by the Ministry of Electronics and Information Technology is attached herewith as **ANNEXURE-1 (pp. 8-9)**

3. That in the lockdown, the Hon'ble Supreme Court, High Courts and Subordinate Courts have by and large remained shut. Few hearings are taking place through video conferencing. Few High Courts like Kerala High Court and Bombay High Court have live streamed these proceedings, while others, including the Hon'ble Supreme Court have not done so. All the Courts as well as Government Departments are using different software for hearing through video conferencing. These range from WhatsApp to Skype to Zoom applications.

   True Copy of Chart showing List of Video Conferencing Software being used by Courts and Government Departments is attached herewith as **ANNEXURE-2. (pp 10-13)**

4. That this Hon'ble Court on 06 April 2020 in Suo Motu Writ (Civil) No 5/2020, passed certain directions regarding guidelines for court functioning through video conferencing during COVID-19 pandemic. In the said Order, this Hon'ble Court said, "every High Court is authorised to determine the modalities which are suitable to the temporary transition to the use of video conferencing technologies".
5. That it is true that a unique situation requires unique solutions, but the same cannot be at the altar of Rule of Law. It is submitted that most of the Video Conferencing Software being used are products of foreign internet companies, with their terms of use mandating transfer of data outside India as well as its commercial exploitation.

   True Copy of Extract of Terms of Use of Video Conferencing Software showing transfer of data outside India and commercial usage is attached as **ANNEXURE-3 (pp 14-22).**

6. That the Petitioner most humbly submits that the transfer of data, especially governmental and judicial data outside India impacts national security and contravenes the Public Records Act, 1993, the Official Secrets Act, 1923, the Email Policy as well as Policy for usage of IT Resources of the Government of India. It is submitted that the transfer of data, which inevitably takes place as a result of use of foreign based video conferencing software, might assist, directly or indirectly, an enemy or might prejudicially affect the sovereignty and integrity of India, the security of the State or friendly relations with foreign States. In fact, the Email Policy as well as Policy for usage of IT Resources was made by the Government as result of the Writ Petition (Civil) 3672/2012 filed by the Petitioner before the Delhi High Court.

True Copy of Extracts from Public Records Act, 1993, Email Policy and Policy on use of IT Resources is attached herewith as **ANNEXURE-4 (pp. 23-27).**

7. That on 12 April 2020, the Ministry of Home Affairs vide its Cyber Coordination Centre has issued an advisory on Zoom video conferencing software being unsafe.

   True Copy of Ministry of Home Affairs Advisory on Zoom App is attached herewith as **ANNEXURE-5 (pp. 28-43).**

8. That on 15 April 2020, the Computer Emergency Response Team (CERT-IN) has also issued an advisory in relation to video conferencing platforms. In the said advisory, CERT has said that "Fraudsters have found…opportunity to conduct unauthorized activities resulting in obtaining of sensitive information of individuals and organization".

   True Typed Copy of CERT-IN ADVISORY CIAD-2020-0020 dt. 15.04.2020 is attached herewith as **ANNEXURE-6 (pp. 44-46).**

9. That the Judges and the Ministers take oath as per Schedule III of the Constitution. The Ministers to the Government also take the oath of Secrecy, which binds them to "not directly or indirectly communicate or reveal to any person or persons any matter which shall be brought under...consideration or shall become known to …a Minister for the Union except as may be required for the due discharge of...duties as such Minister"

10. That no transfer of governmental data, without permission, is permitted. As a result of usage of the foreign based video conferencing software, several officials have become liable for punishment under the Section 9 of Public Records Act, 1993, which mandates imprisonment and fine. The Petitioner most humbly submits that such action on public officials will

be unwarranted. Nevertheless, adequate legal and technological solutions are required to preserve the Rule of Law.

11. That the institutions using video conferencing facilities may be required to keep a copy of the same under the Right to Information Act, 2005. Moreover, it is rather ironic that photos of the Union Defence Minister using Zoom video conferencing software to talk to the Chief of Defence Staff were posted on the official Twitter handle. Similarly, questions have been raised about data security of WhatsApp and other similarly placed applications.
12. That, the above shows that allowing transfer of government data abroad has implications on national security as well as constitutional and legal ramifications.
13. That important meetings like those of the Cabinet have may secretive contents, which should not come out in the public. India is always a target of terrorism and needs to take special care to avoid any attack, be it traditional, biological or technological.
14. That it is submitted that the video conferencing and live streaming infrastructure should be treated as “critical information infrastructure” and their security must be audited by appropriate government agencies as per Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.
15. That it would be best to utilize video-conferencing software provided by the National Informatics Centre (NIC) for functioning of the Government and the Judiciary. In case such sophisticated software made by NIC is not readily available,

then suitable software from a private vendor may be audited by NIC, and be certified for usage by the Government and the Judiciary.

PRAYER

It is therefore prayed that this Hon'ble Court may be pleased to:

a) Direct the Respondents to provide NIC based infrastructure/NIC audited infrastructure for communication and video conferencing for Judiciary and all government officials;

b) Direct the requisite amendment in the Supreme Court Rules, 2013 and Rules of the High Courts as per Order dated 06.04.2020 in Suo Motu Writ (Civil) No 5/2020, with necessary safeguards for hearing through video conferencing;

c) Pass further order(s) as may be deemed fit and proper fit in light of above facts and circumstances or the interest of justice;

Drawn by **Filed by**

Sachin Mittal and Gaurav Pathak, Advocates

Sachin Mittal
Advocate for the Petitioner

Drawn on: 17.04.2020

Filed on: 18.04.2020

IN THE SUPREME COURT OF INDIA
CIVIL ORIGINAL JURISDICTION
WRIT PETITION(C) NO 1016 OF 2019

IN THE MATTER OF:-

K.N. GOVINDACHARYA …PETITIONER

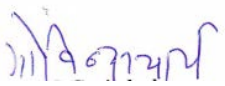
VERSUS

SECRETARY GENERAL & ORS. …RESPONDENTS

AFFIDAVIT

I, K.N. Govindacharya, S/o Lt. Sh. K. V. Neelameghacharya aged about 76 years, R/o House No. 8313, Sector-C, Pocket 8, Vasant Kunj, New Delhi-110070 do hereby solemnly affirm and state as follows:-

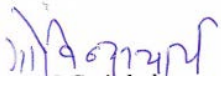
1. That I am the Petitioner in the aforesaid matter and am conversant with the facts and circumstances of the case and am competent to swear this affidavit.
2. That I have read and understood accompanying application from para 1 to 15, pages 1 to 6 , and do state that the facts stated therein are true and correct to the best of my knowledge.
3. That the Annexures 1-5 are true copy/true typed copy of their originals.
4. That the Petitioner has no personal gain, private motive or oblique reason in filing the PIL.
5. That it is in the interests of justice that the Petitioner's signature in vernacular in Devnagari script in Hindi may be accepted as English translation for the purpose of hearing of the instant petition.



DEPONENT

VERIFICATION

I, the deponent above named do hereby verify that averments made in this affidavit are true and correct to the best of my knowledge and belief. No part of it is false and nothing material has been concealed therefrom. Verified at New Delhi on this the 17th day of April 2020.



DEPONENT

ANNEXURE-1

F.No. 17(4)/2020-Pers.I (Pt)

Government of India

Ministry of Electronics & Information Technology

(Personnel Division)

Dated: 24.03.2020

Sub: Protocol for Work From Home (WFH)

The facility of Work From Home (WFH) has been given to employees who can access the e-office from their respective homes w.e.f 25th March 2020 until further orders. This is done for protecting them (and others) from possible infections. Protecting the health of the employees is of paramount important to Govt.

2. While health of the employees is important, maintaining the employee productivity while on WFH is a non-negotiable. The WFH facility shall not be considered as 'paid leave' (except in case of MTS) and it I expected that the officers who have taken this facility are alert and always available for official functioning remotely. Those official who still do not have the facility of remote access, should immediately contact Shri J.P. Gupta, Sr. Technical Director , NIC Cell , MeitY.

3. In this context, the following protocol will be strictly applied starting from 25th March until further orders:

A. Every working day, before 10AM, each officer on WFH shall fix targets/specific work for their immediate subordinate to be achieved on the day. This shall be sent through eoffice/email (not by phone). The recipient of this e-file/mail shall further allocate work to his/her subordinate (and so on). This correspondence shall be available on eoffice.

B. On the receipt of the work, each employee shall acknowledge to the reporting officer the receipt of work using eoffice network. This communication shall be received before 10:30 AM.

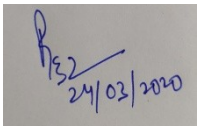
C. Every Employee shall be available for telephonic consultation during office hours and phone shall be answered all the time.

D. In case of any issue that needs consultation, officers can set up remote-meeting (RM) either through the phone or through a WhatsApp Video Call (VC). The notice for such remote-meeting shall preferably be communicated at least one hour in advance. Everyone who is called for VC/RM shall necessarily attend.

E. Every employee on WFH shall dispose off all the receipts and files in their eoffice before 5 PM each day. This shall be monitored by a daily report showing unattended receipts/files.

4. The new system of working shall be used by one and all for improving the productivity at work.

5. Further, if any work (like submission of Bills etc) calls for physically coming to the office, they shall come for that specific work. The office will make suitable arrangement for their transportation.



(Roop Kishor)

Director (Pers)

To,

All GCs

2. DG(NIC)/DG(STQC)

3. CEO(UIDIA)/DG(ICERT)/CCA

4. CEO (DIC)/CEO(NeGD)/CEO(MyGov)

5. OSD to Secretary

6. PPS to AS(GS)

ANNEXURE-2

VIDEO CONFERENCING APPLICATIONS BEING USED BY JUDICIARY

S. No	INSTITUTION	VIDEO CONFERENCING APPLICATION
1.	Supreme Court	Vidyo[1] and Skype, WhatsApp, Facetime in case of network issues with Vidyo[2]
2.	High Court of Allahabad	Jitsi Meet[3]
3.	High Court of Andhra Pradesh	Zoom[4]
4.	High Court of Bombay	Zoom[5]
5.	High Court of Calcutta	Vidyo[6], earlier it was Microsoft Teams[7]
6.	High Court of Chhattisgarh	Vidyo, switched from Zoom[8]
7.	High Court of Delhi	Cisco WebEx[9]
8.	High Court of Gauhati	Vidyo[10]
9.	High Court of Gujarat	Zoom[11]
10.	High Court of Jammu & Kashmir	WhatsApp Video Calls in case of unavailability of VC[12]
11.	High Court of Jharkhand	Vidyo[13]
12.	High Court of Karnataka	Zoom[14] and Skype[15]
13.	High Court of Kerala	Zoom and WhatsApp[16]
14.	High Court of Madhya	Vidyo[17]

	Pradesh	
15.	High Court of Madras	Zoom[18]
16.	High Court of Manipur	Vidyo[19]
17.	High Court of Meghalaya	Vidyo[20]
18.	High Court of Orissa	Vidyo and WhatsApp calling as an alternative[21] Stopped the use of Zoom[22]
19.	High Court of Patna	Vidyo[23]
20.	High Court of Rajasthan	Jisti Meet[24]
21.	High Court of Sikkim	Vidyo[25]
22.	High Court of Telangana	Zoom[26]
23.	High Court of Tripura	Zoom and Vidyo[27]
24.	High Court of Uttarakhand	Jitsi Meet[28]

[1] https://main.sci.gov.in/pdf/LU/15042020_134922.pdf

[2] https://main.sci.gov.in/pdf/cir/26032020_134544.pdf

[3] http://www.allahabadhighcourt.in/event/event_7403_11-04-2020.pdf

[4] http://hc.ap.nic.in/docs/efilingandvc.pdf

[5] https://bombayhighcourt.nic.in/writereaddata/notifications/PDF/noticebom20200415165454.pdf

[6] https://calcuttahighcourt.gov.in/Notice-Files/ECOURT/2705

[7] https://www.calcuttahighcourt.gov.in/Notice-Files/general-notice/2699

[8] http://highcourt.cg.gov.in/noti/2020/noti_16042020.pdf

[9] http://delhihighcourt.nic.in/writereaddata/Upload/PublicNotices/PublicNotice_K81Q1VBLCEI.PDF

[10] http://ghconline.gov.in/General/Notification-15-04-2020.pdf

[11]https://gujarathighcourt.nic.in/hccms/sites/default/files/miscnotifications/Gujarat%20High%20Court%20-%20Hearing%20by%20VC%20-%20Press%20Note%2024032020(signed).pdf

[12]http://jkhighcourt.nic.in/doc/upload/orders&cir/Circular%2014%20Dated%2023.03.2020.pdf

[13] https://jharkhandhighcourt.nic.in/node/display_pdf/SOP_VC11042020

[14] https://karnatakajudiciary.kar.nic.in/noticeBoard/final%20e-filing-circular.23.3.2020.pdf

[15] https://www.livelaw.in/pdf_upload/pdf_upload-371590.pdf

[16] http://highcourtofkerala.nic.in/downloads/instructions_4adv28032020.pdf

[17] https://mphc.gov.in/PDF/web_pdf/LU/CamScanner%2004-16-2020%2015.03.12.pdf

[18] https://timesofindia.indiatimes.com/city/chennai/madras-high-court-zooms-into-era-of-digital-hearing-seamlessly/articleshow/75040585.cms

[19] https://hcmimphal.nic.in/documents/Checkpoints%20email%20filing.pdf

[20] http://meghalayahighcourt.nic.in/sites/default/files/c7_0.pdf

[21] https://www.orissahighcourt.nic.in/important-notices-pdf-view/notification/192/

[22] https://www.orissahighcourt.nic.in/important-notices-pdf-view/notification/196/

[23] http://patnahighcourt.gov.in/pdf/UPLOADED/3562.PDF

[24] https://hcraj.nic.in/hcraj/Allfiles/JitsiSOP.pdf

[25] https://highcourtofsikkim.nic.in/hcs/sites/default/files/Notification/2020-03-24_3.pdf

[26] http://hc.ts.nic.in/documents/admin_2_2020_03_27_17_50_19.pdf

[27] http://thc.nic.in/notification/7086-7118.pdf

[28] https://highcourtofuttarakhand.gov.in/files/SOP_12042020_1.pdf

ANNEXURE-3

TERMS OF USE OF VIDEO CONFERENCING SOFTWARE USED

A. VIDYO APP (https://www.vidyo.com/privacy-policy)

1. When you use a Vidyo product or service either as a Customer, a registered User under a Customer's account, or a guest of a Customer or registered User, Vidyo may automatically collect and store certain information about your usage of and interaction with Vidyo's products and services such as server information (hardware settings and statistics, network information, system activity, server configuration, alerts, utilization, appliance version, browser details) and call records ("CDRs") which contain the time and duration of calls, the number and types of participants on each call, and electronic identification data of the call participants such as user name (which may be the participant's email address), display name, IP address, telephone number (if the participant joined by telephone), server details, endpoint type and version, device type and type and version of operating system, browser type, version and language, and circumstances of disconnecting from the call. In addition, Vidyo may collect certain endpoint information (such as hardware statistics, network information, application settings, log files, error reports and usage).

2. When you access a Vidyo product or service from a smart phone, tablet or other mobile device, the mobile services

provider may transmit to us uniquely identifiable mobile device information which may include, or may allow us to determine, information such as your operating system version, language and time zone, system activity, usage activity, and network information.

3. Some of our products or services may at the Customer's election, include a feature allowing a participant to record the content of video conferences and instant messaging communications. If such feature is used, a notice will appear on your screen and in such case, we may collect and store the content of such video conferences and instant messaging communications.

4. We may use collected information to comply with legal or governmental requirements or demands.

5. Electronic information collected by Vidyo is kept on servers that are owned or operated either by Vidyo or by Vidyo contracted suppliers. These servers are predominantly located in the United States, Europe and Asia. We ensure that we comply with the applicable legal requirements when transferring your personal information outside the European Economic Area ("EEA").

6. We use certain tracking scripts on Our Websites, including Google Analytics, Bizable, and Marketo for analytics and tracking purposes. When you use Our Websites or Vidyo products and services, we may also employ web beacons (also known as clear GIFs) which are used to track the

online usage patterns of users of Our Websites or Vidyo products or services.

7. We currently do not participate in any "Do Not Track" frameworks that would allow us to respond to signals or other mechanisms from you regarding the collection of your information.

8. Vidyo may share your information as follows:
   - With our subsidiaries and controlled affiliates located in the U.S. or elsewhere, as we believe necessary for business purposes;
   - With our suppliers and Channel Partners, under appropriate non-disclosure and data security obligations for purposes of providing products or services to us or distributing our products and services
   - With government authorities or other third parties when Vidyo believes such action is necessary or desirable to respond to legal process or government demands; to protect our Customers or Users; to protect lives or property rights; or to maintain the security of our products or services; and
   - Customer and User information in Vidyo's files may be transferred in a corporate reorganization transaction such as a sale or divestiture of the company or its assets. We may also transfer or assign such information in the course of a bankruptcy, dissolution or similar transactions or proceedings.\

B. SKYPE (https://www.skype.com/en/legal/)

1. Device and usage data. Data about your device and the product and features you use, including information about your hardware and software, how our products perform, as well as your settings. For example:

- Payment and account history
- Browse history
- Device, connectivity, and configuration data.
- Error reports and performance data
- Troubleshooting and help data
- Bot usage data

2. Voice data. Your voice data, such as the search queries or commands you speak, which may include background sounds.

3. Location data. Data about your device's location, which can be either precise or imprecise. For example, we collect location data using Global Navigation Satellite System (GNSS) (e.g., GPS) and data about nearby cell towers and Wi-Fi hotspots. Location can also be inferred from a device's IP address or data in your account profile that indicates where it is located with less precision, such as at a city or postcode level.

4. Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the

content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

5. Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

6. We share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement.

C.

WHATSAPP (https://www.whatsapp.com/legal/#privacy-policy-information-we-collect)

1. Usage and Log Information. We collect service-related, diagnostic, and performance information. This includes information about your activity (such as how you use our Services, how you interact with others using our Services,

and the like), log files, and diagnostic, crash, website, and performance logs and reports.

2. Device and Connection Information. We collect device-specific information when you install, access, or use our Services. This includes information such as hardware model, operating system information, browser information, IP address, mobile network information including phone number, and device identifiers. We collect device location information if you use our location features, such as when you choose to share your location with your contacts, view locations nearby or those others have shared with you, and the like, and for diagnostics and troubleshooting purposes such as if you are having trouble with our app's location features.

3. You share your information as you use and communicate through our Services, and we share your information to help us operate, provide, improve, understand, customize, support, and market our Services.

D. ZOOM (https://zoom.us/privacy)

Data collected by us are:

1. Customer content: information you or others upload, provide, or create while using Zoom, such as Cloud recordings, chat / instant messages, files, whiteboards, and other information shared while using the service, voice mails

2. Technical information about your devices, network, and internet connection such as IP address, MAC address, other device ID (UDID), device type, operating system type and version, client version, type of camera, microphone or speakers, connection type, etc.

3. Setting and preferences chosen by the user such as Join with video off, require meeting password, Enable waiting room, Do not allow screen sharing other than host.

4. Metdata such as Duration of the meeting / Zoom Phone call, Email address, name, or other information that a participant enters to identify themselves in the meeting, Join and leave time of participants, Name of the meeting, Date / time that meeting was schedule, Chat status (unless a setting is actively chosen by user), Call data records for Zoom Phone.

5. If you attend a Zoom meeting or webinar as a participant, the host may choose to record the session, and if so, the host is responsible for obtaining consent from you. Recordings may contain personal data and may be stored in Zoom's cloud at the request of the customer. Zoom Phone allows customers to record phone calls, receive voice mail recordings, and obtain transcripts of voicemail, all which may contain personal information and also be stored in our cloud.

6. To Third Party Service Providers. We use third-party service providers to help us provide portions of the Zoom

services and give support. Examples of these third parties include public cloud storage vendors, carriers, our payment processor, and our service provider for managing customer support tickets. They only receive data needed to provide their services to us. We have agreements with our service providers that say they cannot use any of this data for their own purposes or for the purposes of another third party.

E. Microsoft Team (https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4qVL2)

1. CUSTOMER DATA is all data, including text, sound, video, or image files and software, that you provide to Microsoft or that is provided on your behalf through your use of Microsoft online services. For example, it includes data that you upload for storage or processing, as well as applications that you upload for distribution through a Microsoft enterprise cloud service.

2. PERSONAL DATA means any information relating to an identified or identifiable natural person. In other words, personal data is any data that is associated with a specific person. Personal data provided by our customers through their use of online services, such as the names and contact information of customer end users, would also be considered customer data. But personal data could also include certain data that is not customer data, such as the user ID our service assigns to each user; such personal data

is pseudonymized to prevent identification of the individual.

3. To enable cost savings and efficiencies for data storage, Microsoft stores customer data from multiple customers on the same equipment (known as a multitenant architecture). However, we go to great lengths to help ensure that multi-tenant deployments of cloud services such as Office 365, Azure, Dynamics 365, and others logically separate the data (and the processing thereof) of different accounts and support the privacy and security of the data stored

4. Microsoft identifies who can access customer data and the circumstances under which they can access it. Microsoft also logs and reports all access to customer data and other critical data. Additionally, Microsoft and its third-party auditors conduct sample audits to verify that the customer's data is accessed only for appropriate business purposes.

/TRUE COPY/

ANNEXURE-4

EXTRACT OF LAWS GOVERNING CONFIDENTIALITY OF OFFICIAL DATA

Public Records Act, 1993

4. Prohibition against taking of public records out of India.—No person shall take or cause to be taken out of India any public records without the prior approval of the Central Government:

Provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose.

9. Penalty for contraventions.—Whoever contravenes any of the provisions of Section 4 or Section 8 shall be punishable with imprisonment for a term which may extend to five years or with fine which may extend to ten thousand rupees or with both.

Official Secrets Act, 1923

5. Wrongful communication, etc., of information.—(1) If any person having in his possession or control any secret official code or password or any sketch, plan, model, article, note, document or information which relates to or is used in a prohibited place or relates to anything in such a place, or which is likely to assist, directly or indirectly, an enemy or which relates to a matter the disclosure of which is likely to affect the sovereignty and integrity of India, the security of the State or friendly relations with foreign States or which has been made or obtained in contravention of this Act, or which has been entrusted in confidence to him by any person holding office

under Government, or which he has obtained or to which he has had access owing to his position as a person who holds or has held office under Government, or as a person who holds or has held a contract made on behalf of Government, or as a person who is or has been employed under a person who holds or has held such an office or contract—

(*a*) wilfully communicates the code or password, sketch, plan, model, article, note, document or information to any person other than a person to whom he is authorised to communicate it, or a Court of Justice or a person to whom it is, in the interests of the State, his duty to communicate it; or

(*b*) uses the information in his possession for the benefit of any foreign power or in any other manner prejudicial to the safety of the State; or

(*c*) retains the sketch, plan, model, article, note or document in his possession or control when he has no right to retain it, or when it is contrary to his duty to retain it, or wilfully fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or

(*d*) fails to take reasonable care of, or so conducts himself as to endanger the safety of the sketch, plan, model, article, note, document, secret official code or password or information;

he shall be guilty of an offence under this section.

(4) A person guilty of an offence under this section shall be punishable with imprisonment for a term which may extend to three years, or with fine, or with both.

15. Offences by companies.—(1) If the person committing an offence under this Act is a company, every person who, at the time the offence was committed, was in charge of, and was responsible to, the company for the conduct of business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to such punishment provided in this Act if he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any negligence on the part of, any director, manager, secretary or other officer of the company such director, manager, secretary or other officer shall also be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section—

(*a*) "company" means a body corporate and includes a firm or other association of individuals; and

(*b*) "director", in relation to a firm, means a partner in the firm.

Policy on use of IT Resources of Government of India

1.2 For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.3 Misuse of these resources can result in unwanted risk and liabilities for the Government. It is, therefore, expected that these resources are used primarily for Government related purposes and in a lawful and ethical way.

7.1 Users shall refrain from using private e-mail servers from Government network.

7.2 E-mail service authorized by the Government and implemented by the IA shall only be used for all official correspondence. For personal correspondence, users may use the name-based e-mail id assigned to them on the Government authorized e-mail Service.

13. Intellectual Property

Material accessible through the IA's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Government network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

15. Deactivation

In case of any threat to security of the Government systems or network from the resources being used by a user, the

resources being used may be deactivated immediately by the IA.

Email Policy of Government of India

2.1 Only the e-mail services provided by NIC, the Implementing Agency of the Government of India shall be used for official communications by all organizations except those exempted under Clause No. 14 of this policy. The e-mail services provided by other service providers shall not be used for any official communication.

2.2 This policy is applicable to all employees of GoI and employees of those State/UT Governments that use the e-mail services of GoI and also those State/UT Governments that choose to adopt this policy in future. The directives contained in this policy must be followed by all of them with no exceptions.

CyCord One stop shop on all Cyber matters

Cyber Coordination Centre
Government of India

MINISTRY OF HOME AFFAIRS
Government of India

dated April 12, 2020

Advisory on Secure use of Zoom meeting platform by private individuals (not for use by government offices/officials for official purpose)

Zoom is a not a safe platform and advisory of cert-in on the same dated Feb 06, 2020 and March 30, 2020 may kindly be referred. These advisories are available on Cert-In website.

2. Those private individuals who still would like to use Zoom for private purpose may kindly follow the following guidelines.

3. Broad objective of this document is to enable/disable certain settings is to:

- prevent unauthorised entry in the conference room
- prevent an authorised participant to carry out malicious on the terminals of other in the conference.
- Avoid DOS attack by restricting users through passwords and access grant.

4. Most of the settings can be done by login into users zoom account at website, or installed application at PC/Laptop/Phone and also during conduct of conference. However certain settings are possible through certain mode/channel only. For example, ***lock meeting*** can be enabled by administrator only when the meeting has started. This documents explains in details all the security configuration through website, App and through console during the conduct of conference

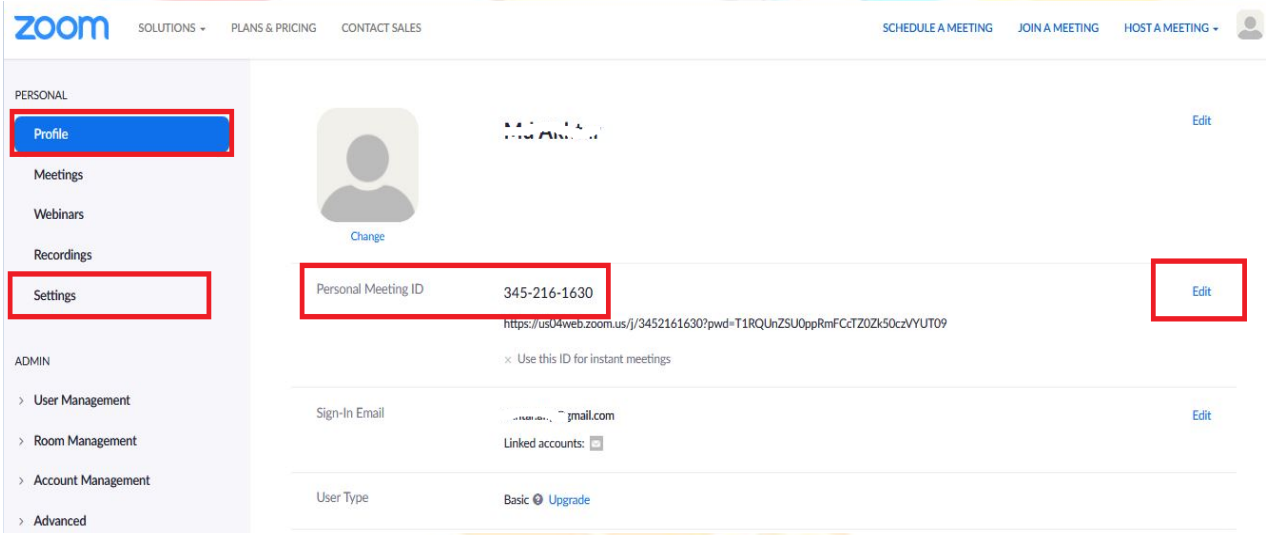
Objective of security configurations:

1. **Setting new user ID and password for each meeting**
2. **Enabling *waiting Room*,** so that every user can enter only when host conducting meeting admits him
3. **Disabling *join before host***
4. Allowing ***Screen Sharing* by host Only**
5. Disabling "***Allow removed participants to re-join"***
6. **Restricting/disabling *file transfer*** option (if not required)
7. ***Locking meeting***, once all attendees have joined
8. Restricting the recording feature
9. To end meeting (and not just leave, if you are administrator)

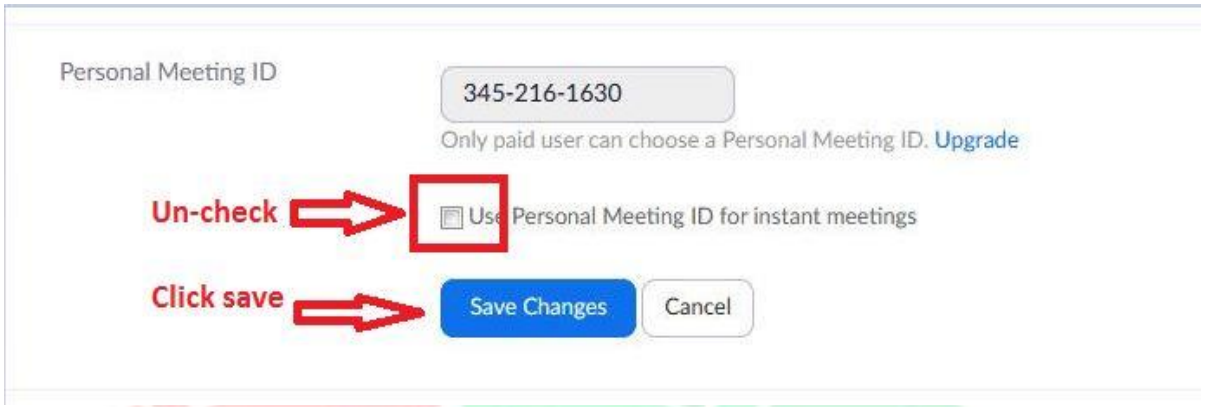
Section 1: Security Configuration Through website

1. Logging into zoom Website: https://zoom.us/ by entering your account credentials

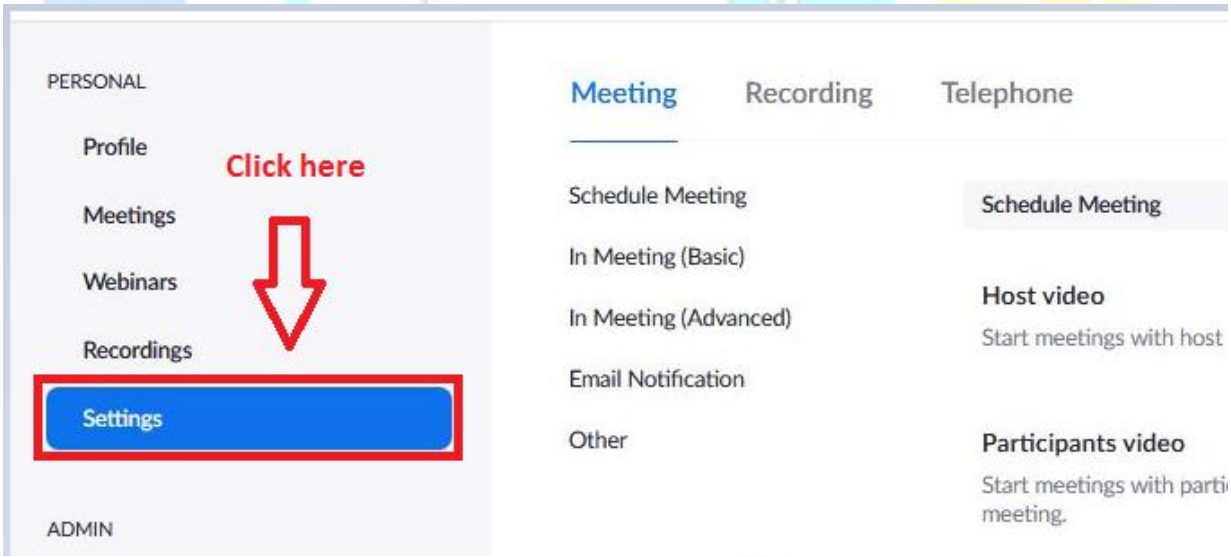
2. After login, page looks like this. Three important and useful links are shown in red boxes, profile, setting and personal meeting ID

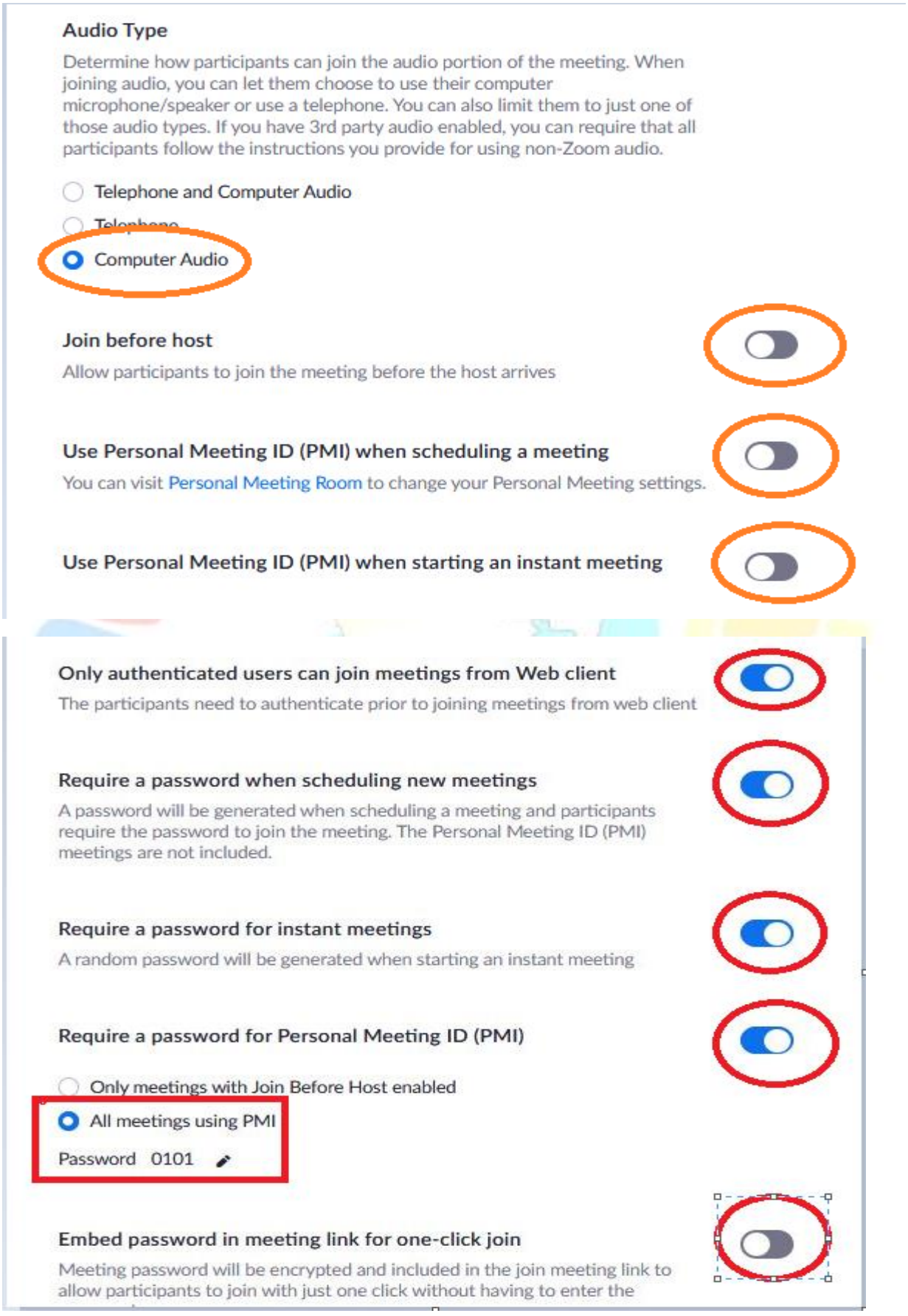


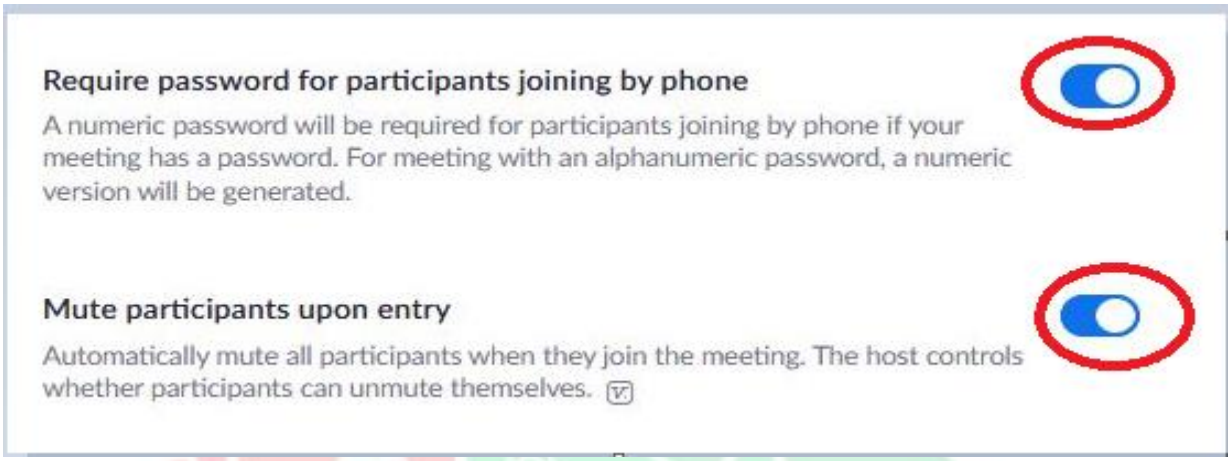
3. Click profile-> edit button in front of personal meeting ID shown in above diagram and un-check the box shown below and click save changes.

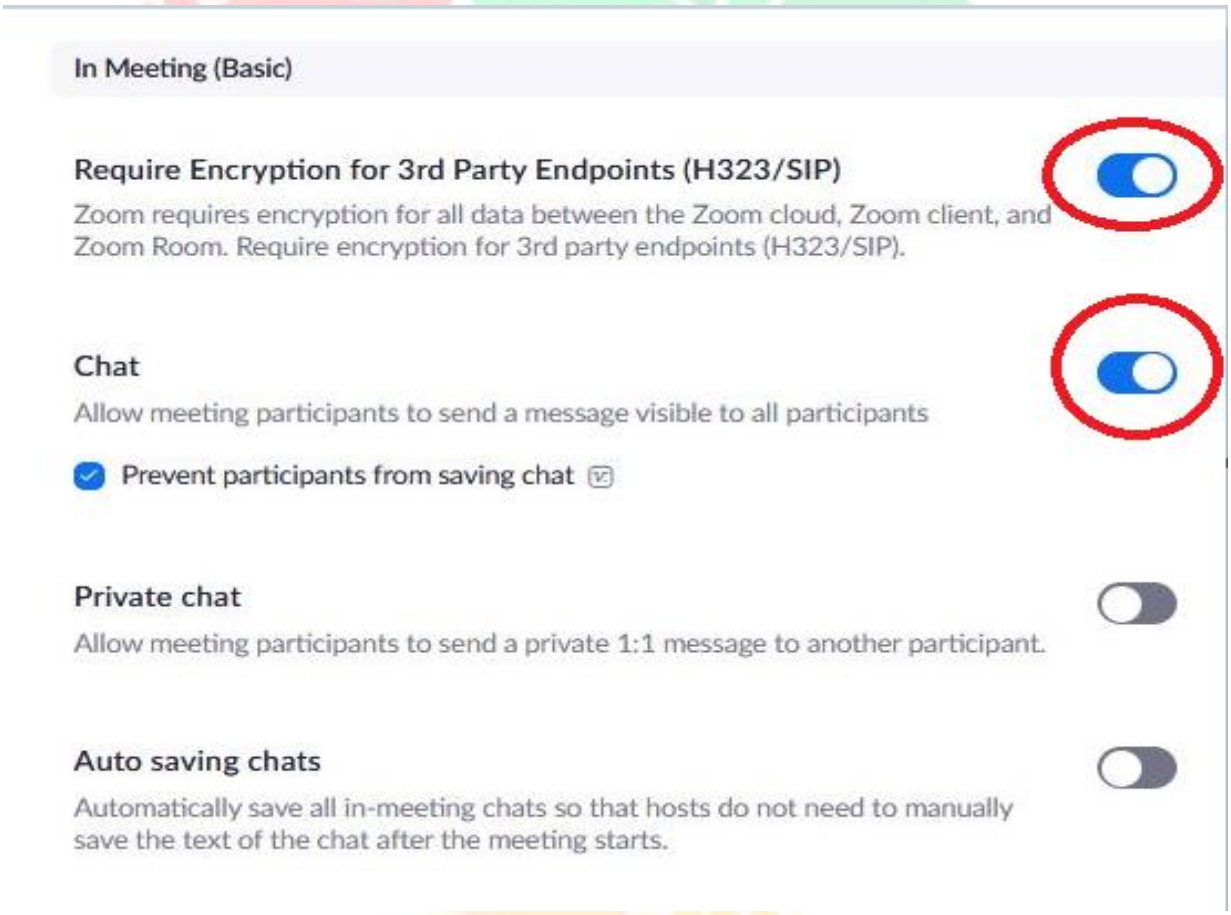


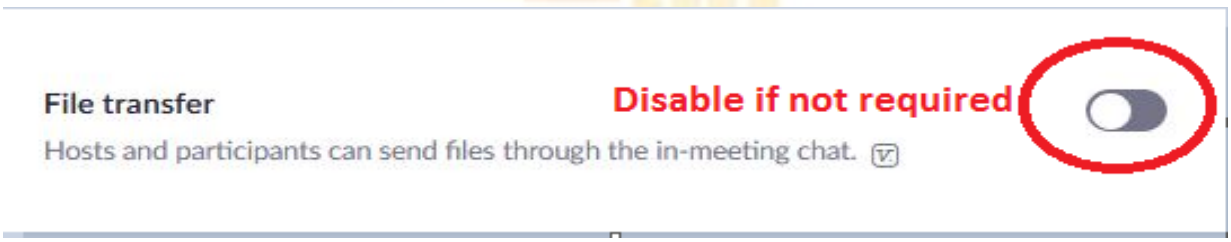
4. Click the setting on home page and keep on scrolling down the window and make necessary configuration as shown in figures below. Only important ones are marked in red boxes and others could be anything

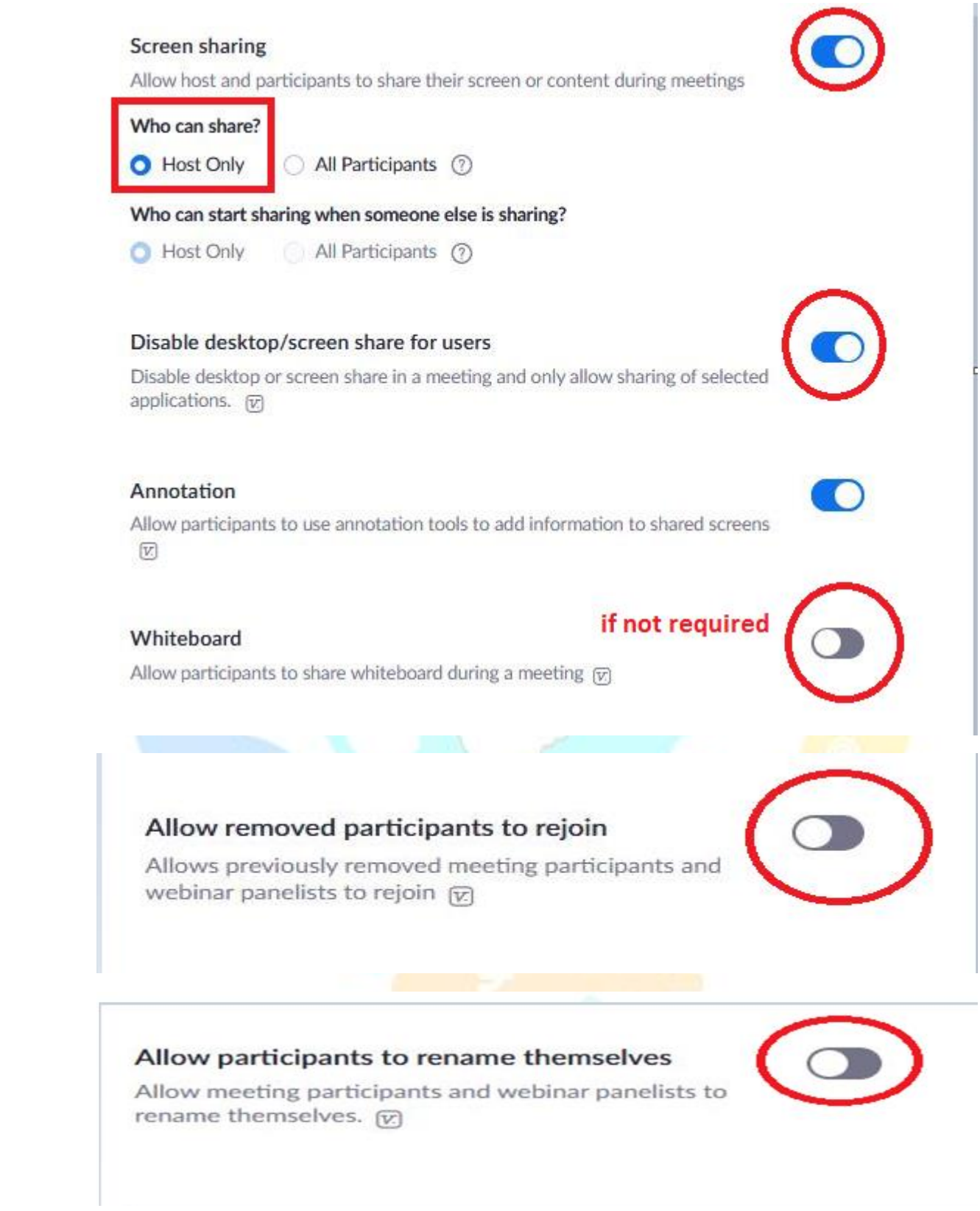


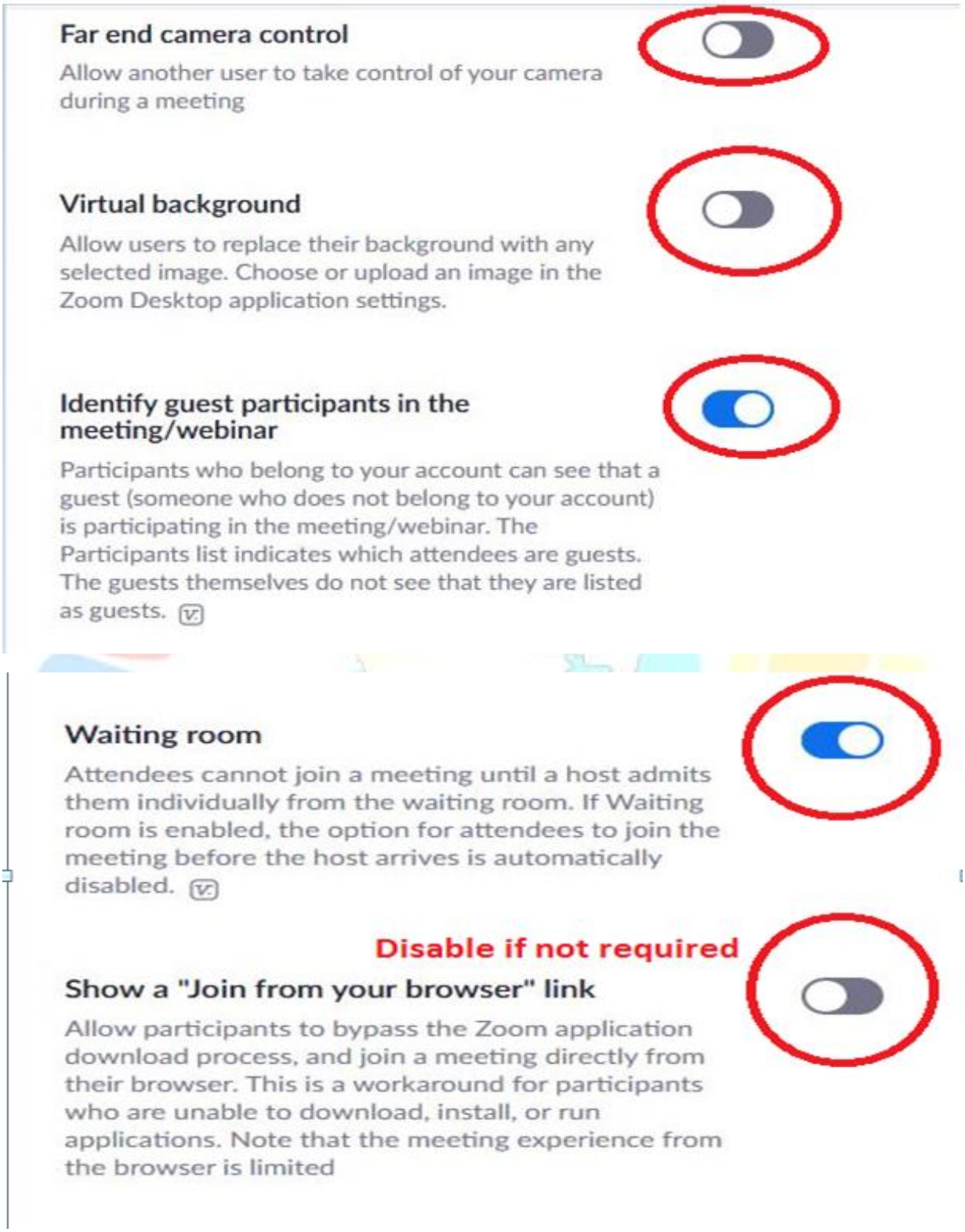

Audio Type
Determine how participants can join the audio portion of the meeting. When joining audio, you can let them choose to use their computer microphone/speaker or use a telephone. You can also limit them to just one of those audio types. If you have 3rd party audio enabled, you can require that all participants follow the instructions you provide for using non-Zoom audio.
Telephone and Computer Audio
Telephone
Computer Audio
Join before host
Allow participants to join the meeting before the host arrives
Use Personal Meeting ID (PMI) when scheduling a meeting
You can visit Personal Meeting Room to change your Personal Meeting settings.
Use Personal Meeting ID (PMI) when starting an instant meeting
Only authenticated users can join meetings from Web client
The participants need to authenticate prior to joining meetings from web client
Require a password when scheduling new meetings
A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.
Require a password for instant meetings
A random password will be generated when starting an instant meeting
Require a password for Personal Meeting ID (PMI)
Only meetings with Join Before Host enabled
All meetings using PMI
Password 0101
Embed password in meeting link for one-click join
Meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the


Require password for participants joining by phone
A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.
Mute participants upon entry
Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.


In Meeting (Basic)
Require Encryption for 3rd Party Endpoints (H323/SIP)
Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).
Chat
Allow meeting participants to send a message visible to all participants
Prevent participants from saving chat
Private chat
Allow meeting participants to send a private 1:1 message to another participant.
Auto saving chats
Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

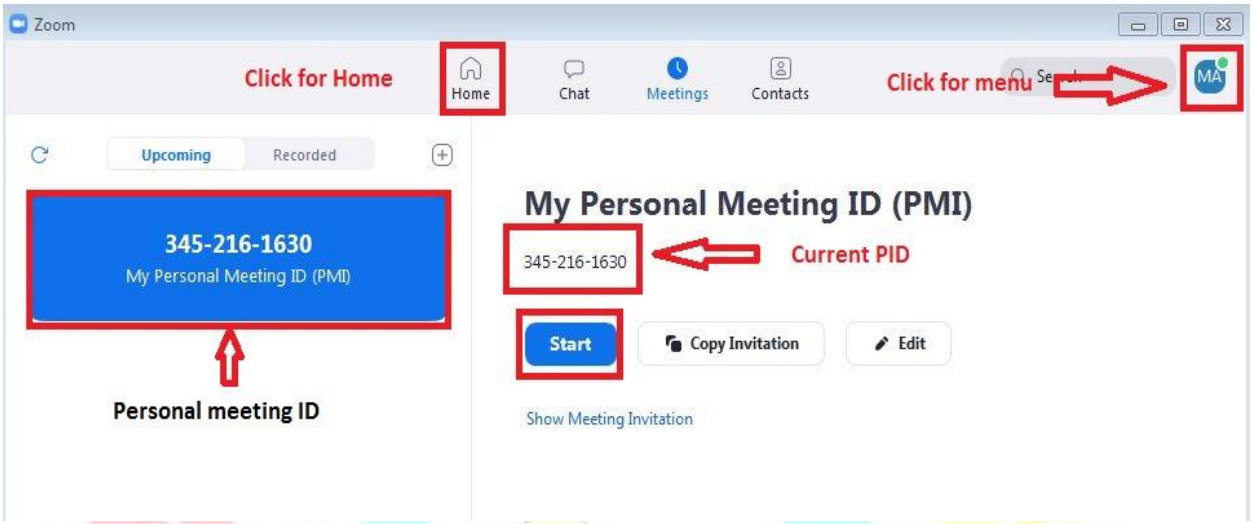

File transfer
Disable if not required
Hosts and participants can send files through the in-meeting chat.


Screen sharing
Allow host and participants to share their screen or content during meetings
Who can share?
Host Only
All Participants
Who can start sharing when someone else is sharing?
Host Only
All Participants
Disable desktop/screen share for users
Disable desktop or screen share in a meeting and only allow sharing of selected applications.
Annotation
Allow participants to use annotation tools to add information to shared screens
Whiteboard
if not required
Allow participants to share whiteboard during a meeting
Allow removed participants to rejoin
Allows previously removed meeting participants and webinar panelists to rejoin
Allow participants to rename themselves
Allow meeting participants and webinar panelists to rename themselves.

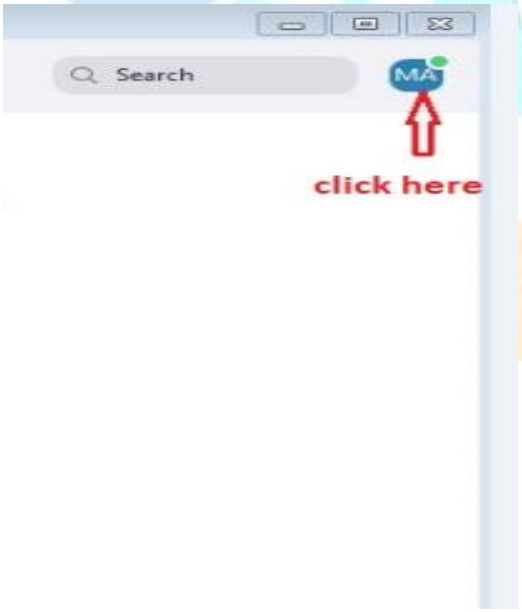

Far end camera control
Allow another user to take control of your camera during a meeting
Virtual background
Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.
Identify guest participants in the meeting/webinar
Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.
Waiting room
Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.
Disable if not required
Show a "Join from your browser" link
Allow participants to bypass the Zoom application download process, and join a meeting directly from their browser. This is a workaround for participants who are unable to download, install, or run applications. Note that the meeting experience from the browser is limited

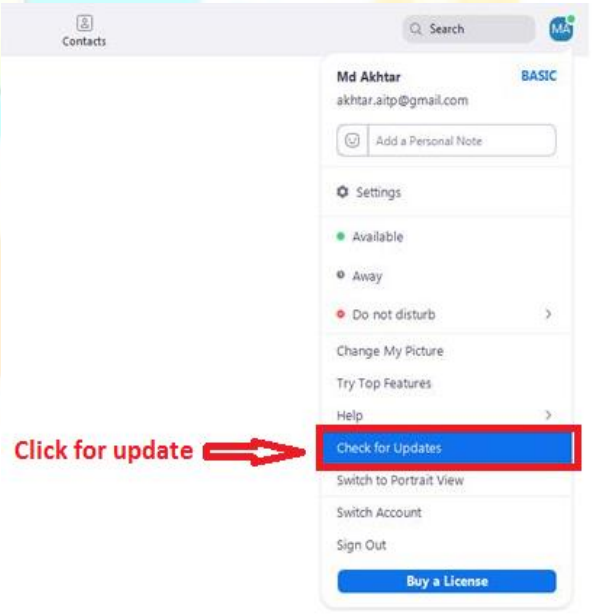
Section 2: Security Configuration Through App

1. Zoom meeting App when launched look like this:

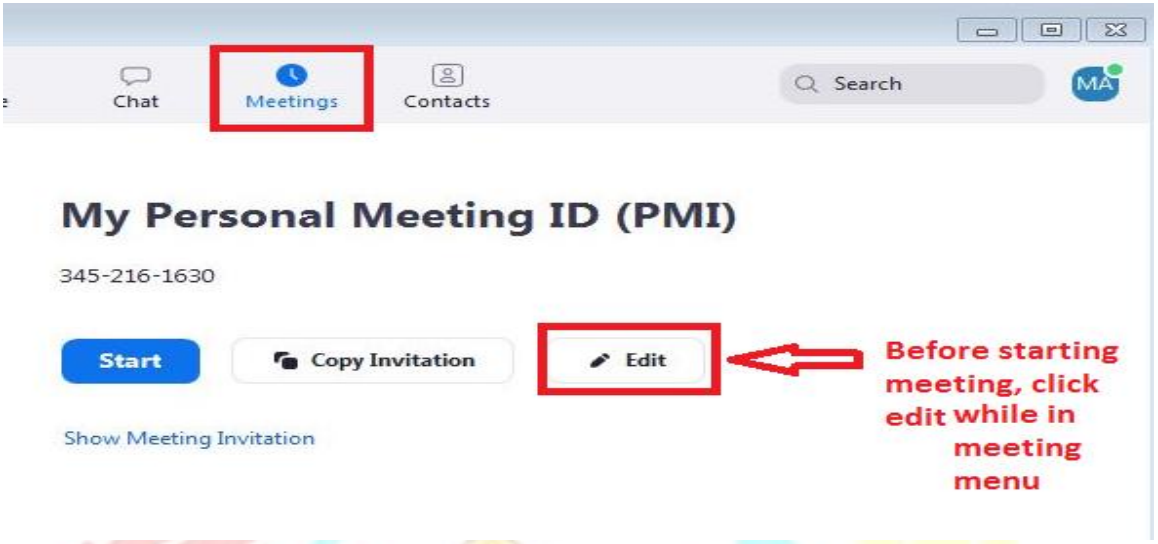


2. **Update your App:** First and fore most important thing is to update your Zoom App:
   - click menu -> navigate to check for update -> click

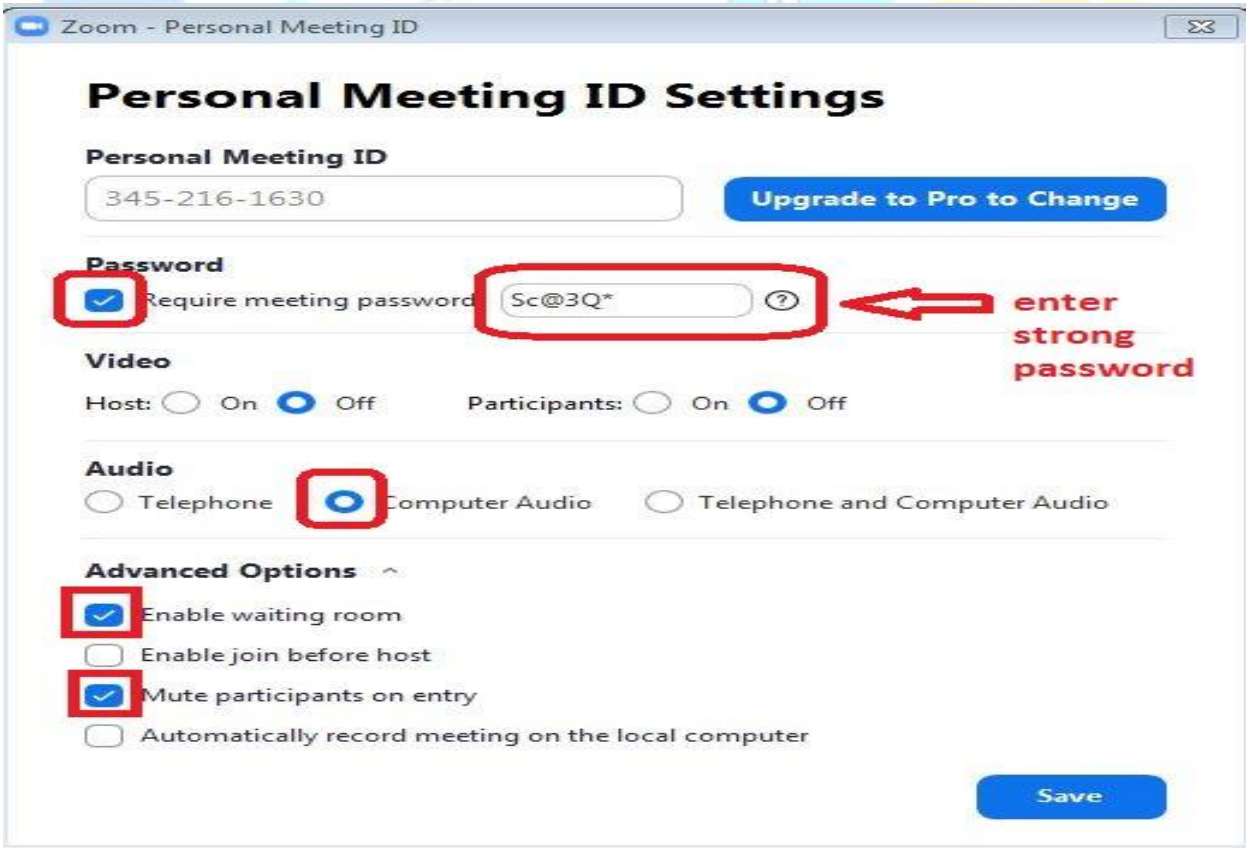




3. **Set a password** for personal meeting ID and **enable waiting**
   - click edit in meeting as shown below

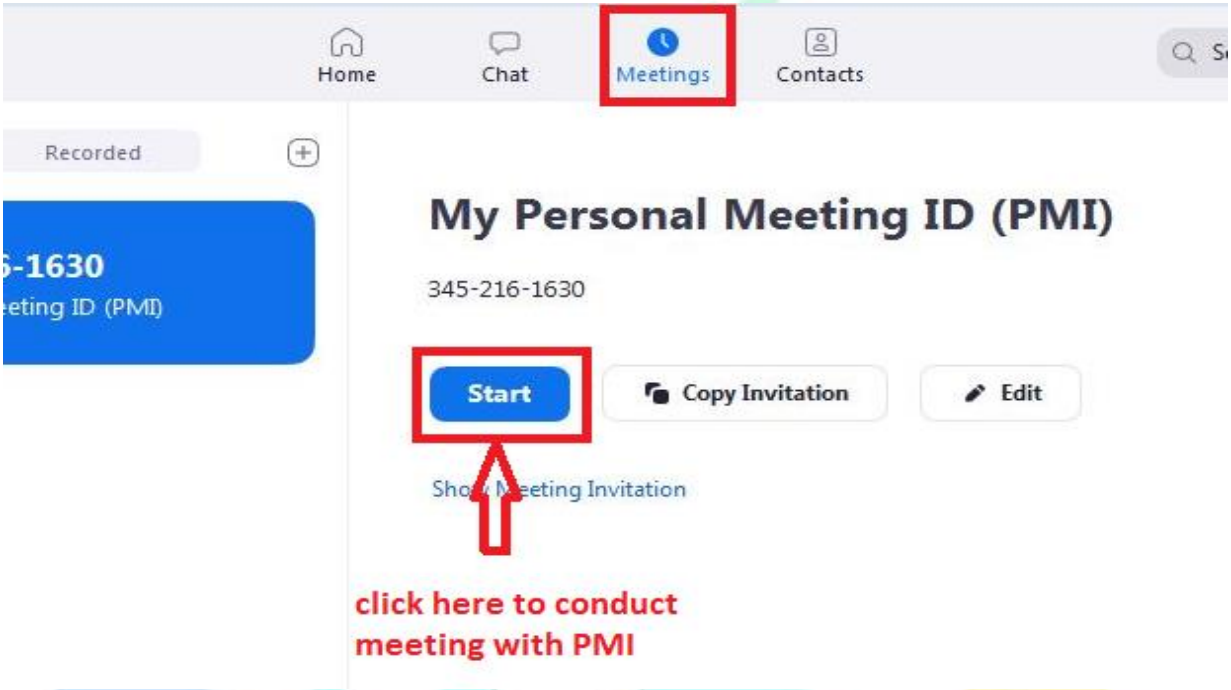


   - Check password box, enter a strong password, check enable waiting window etc. desirable settings are shown in red boxes and click save



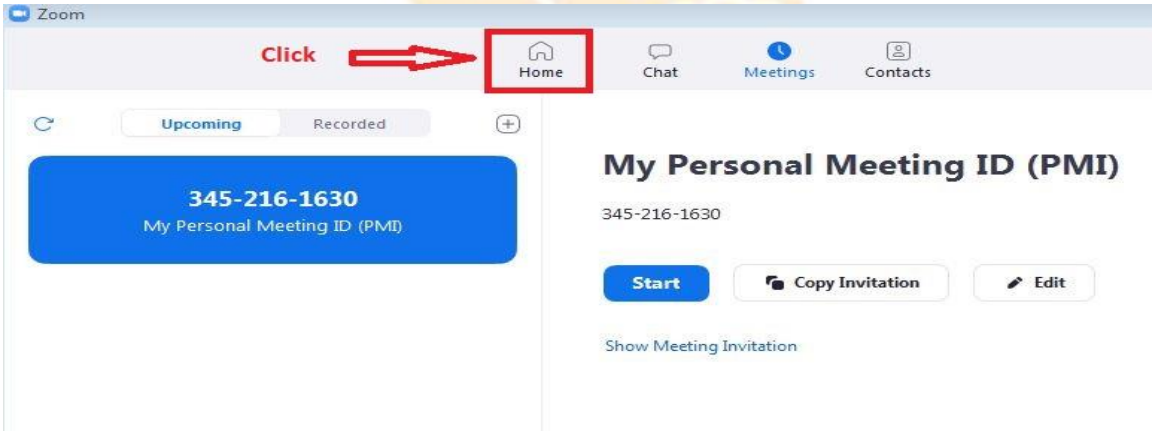
4. **Avoid** conducting meeting by using Personal Meeting ID (PMI).

   Clicking on start as shown below will start a meeting with personal meeting ID and password set by user as shown above. In this case PMI: 3452161630 and password: Sc@3Q*

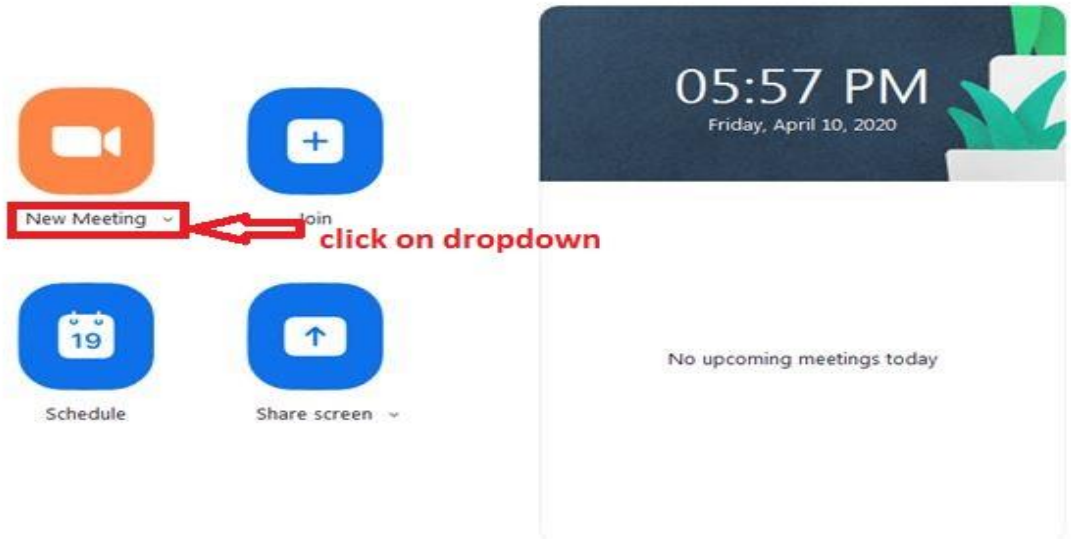


Problem in suing personal meeting ID is that with PMI and password is fixed. It does not automatically change with every new meeting.

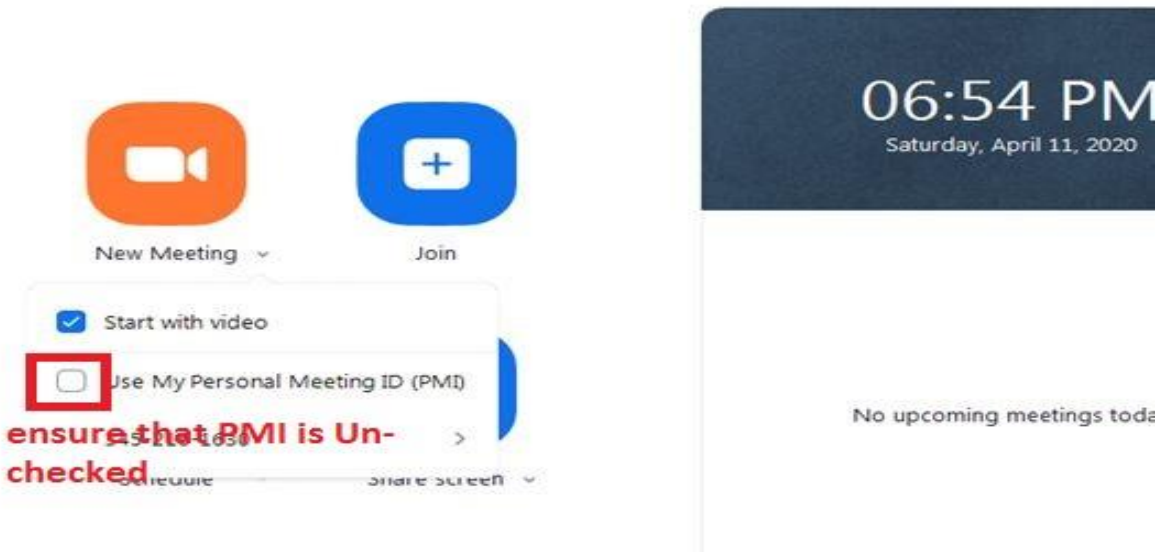
5. **Conduct a new meeting with randomly generated ID and password** instead of fixed one as shown above
   - Click on home



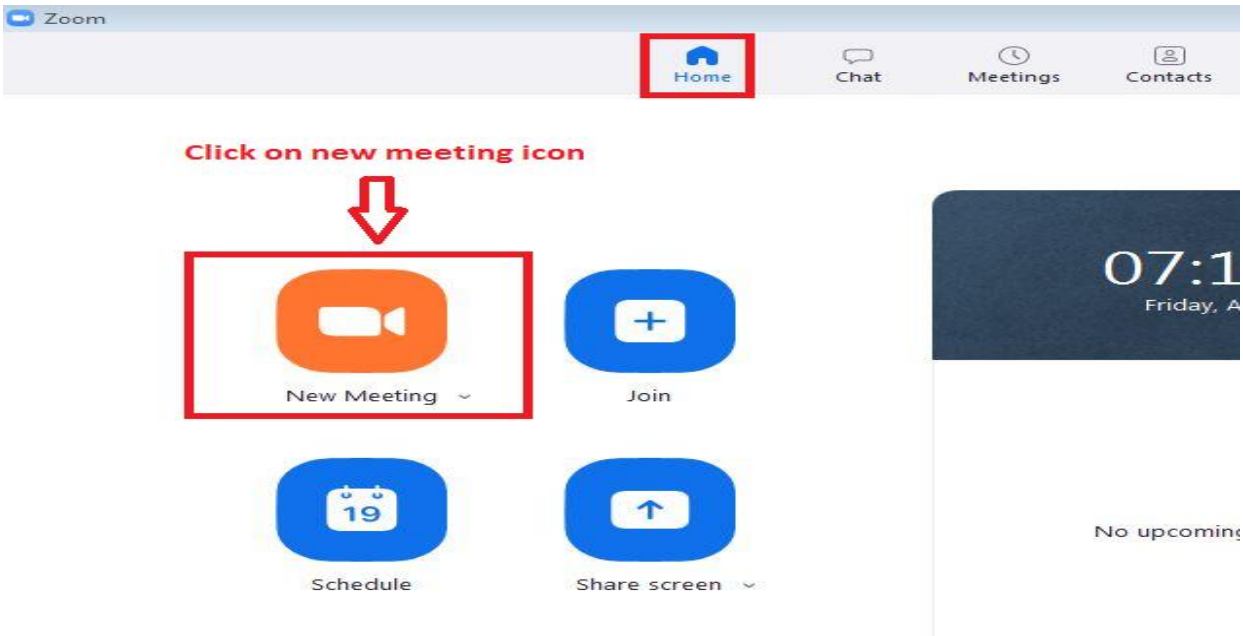
- Click New Meeting drop down as shown below



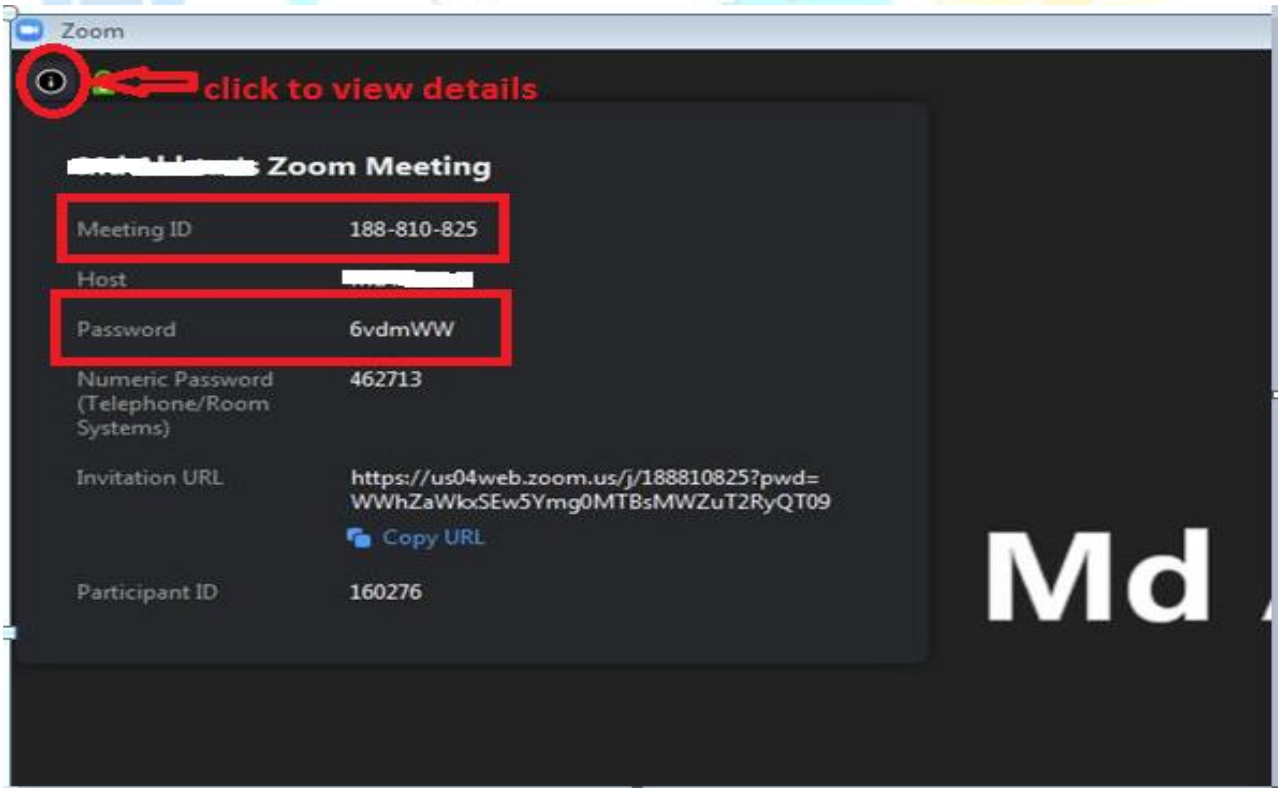
- Un-check use My Personal Meeting ID (PMI), if not already done



- Click new meeting icon to start a new meeting

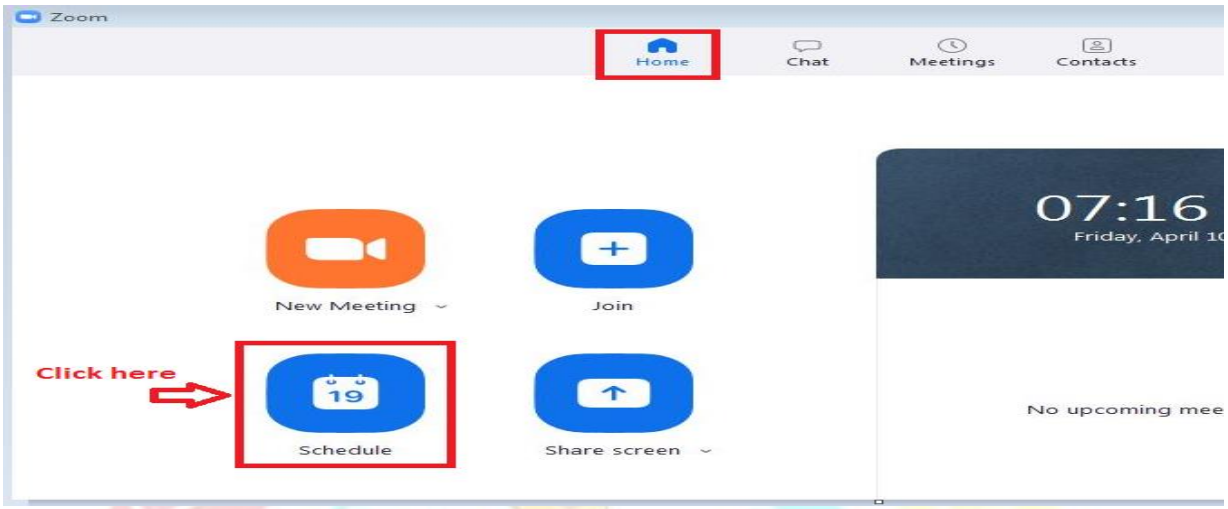


- Once Meeting has started, you will see your meeting ID and password by clicking left top icon below. it will be random and change with every new meeting.

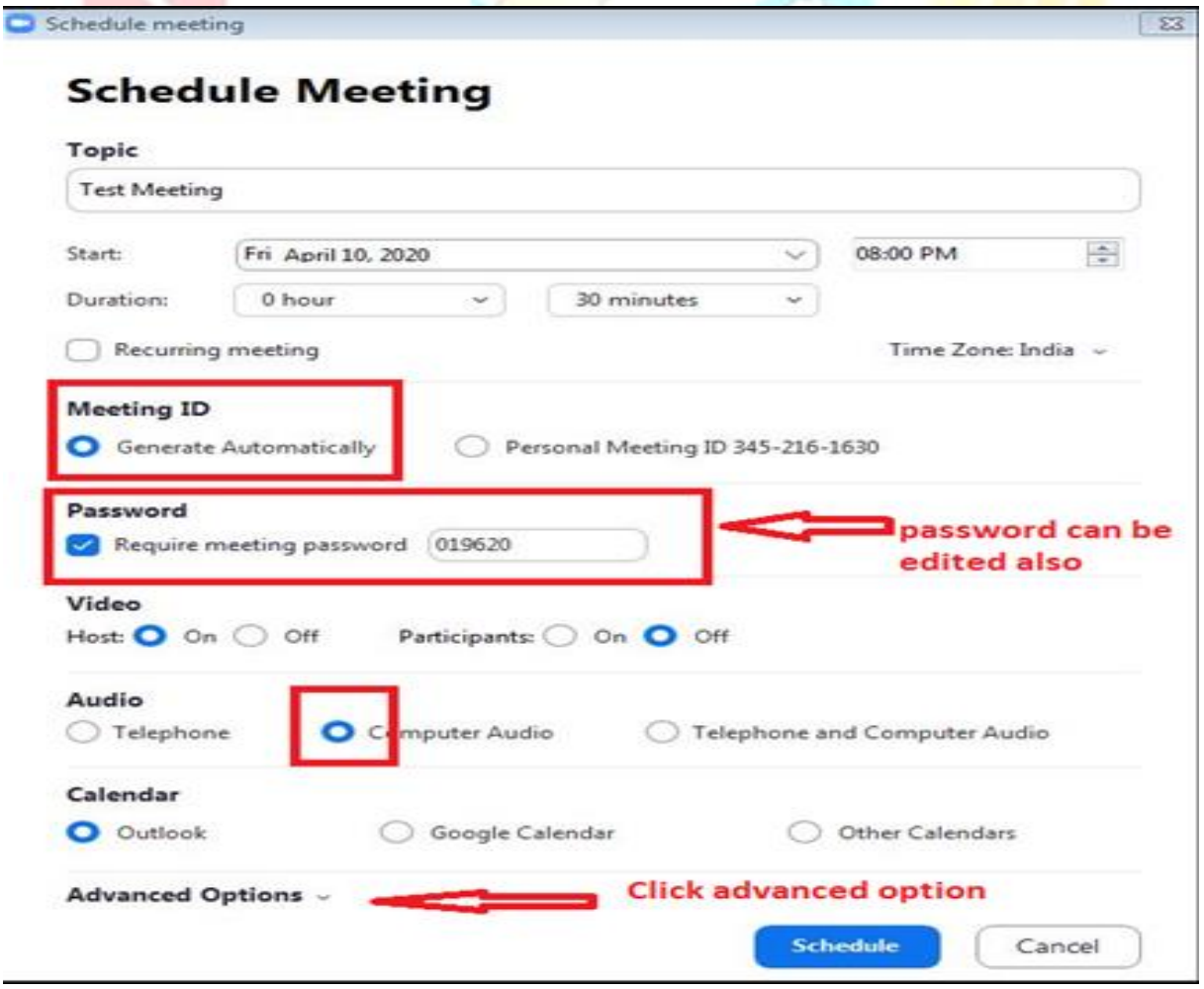


6. Scheduling a meeting with randomly generated ID and password

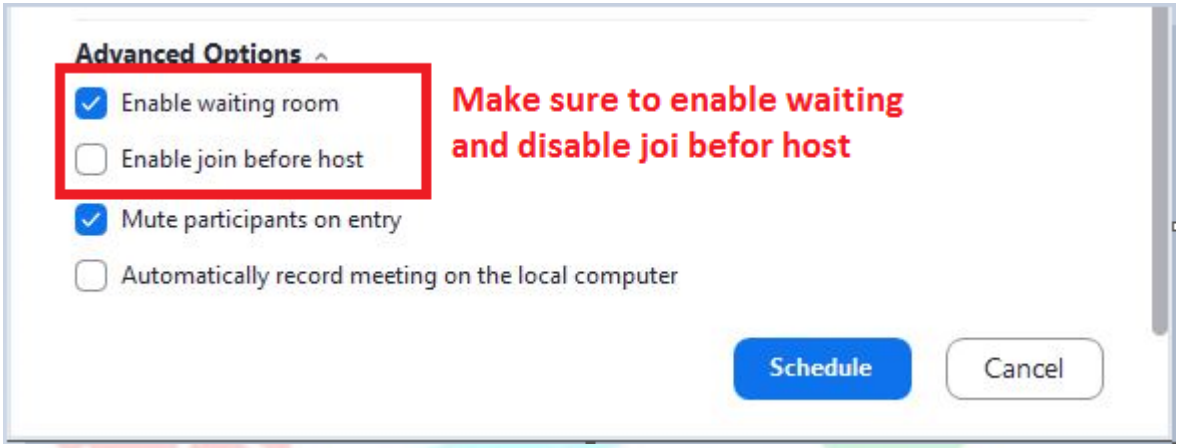
- Click schedule as shown below



- The window as shown below will open up

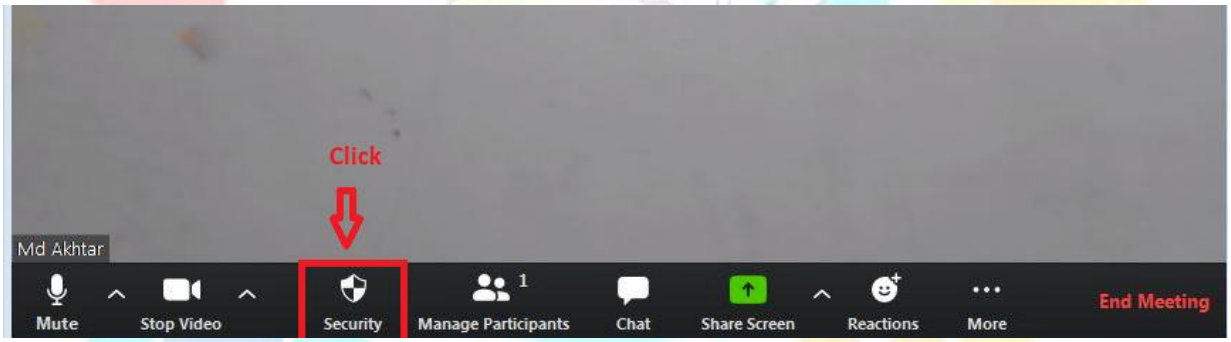


- After clicking ***advanced Options*** shown in above window following expansion will open and do setting as shown below.

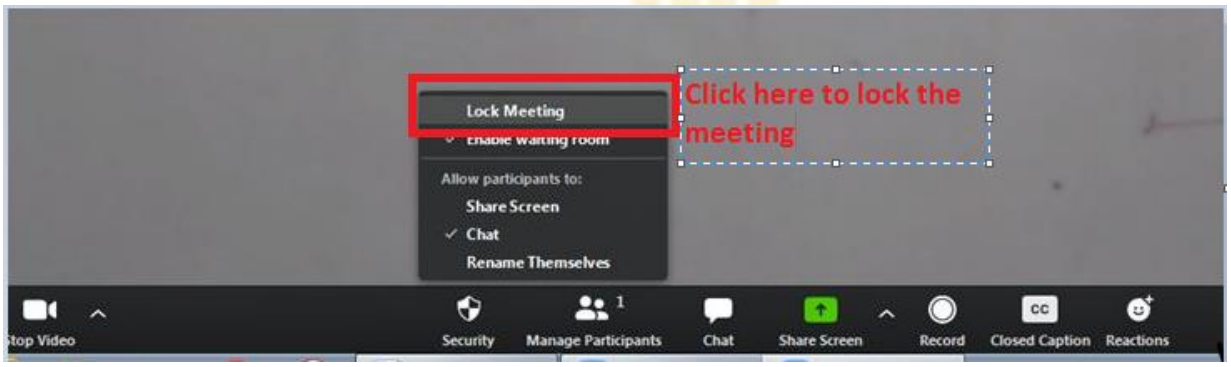


6. **Lock the meeting** session, once all attendees have joined

- Once meeting is in progress, control bar looks like this

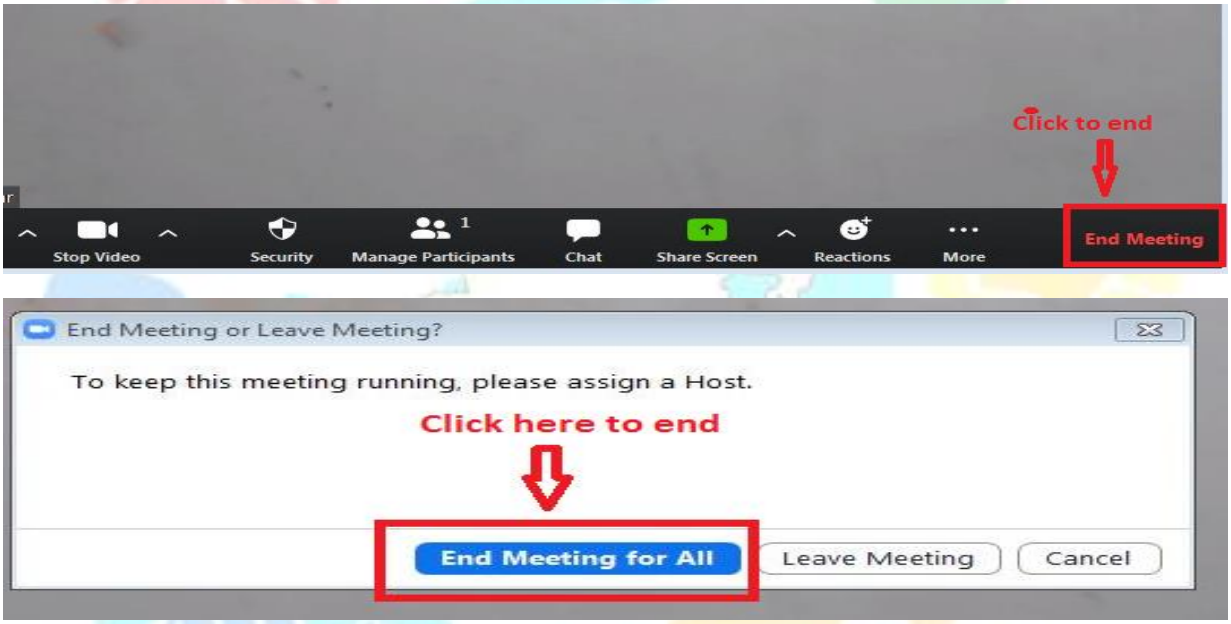


- Click Security and click on Lock Meeting, if all your participants have joined. you can enable waiting room from here also. you can also disable share screen by users from here



Miscellaneous tips:

- Don't use your personal meeting Id (PMI) to host event, instead use randomly generated meeting IDs for each event.
- Don't share your link on public platform, instead share randomly generated meeting id and password for every new meeting session/schedule. It makes it much secure and difficult to leak.
- If you are admin, remember to end meeting, dont just leave meeting.



- Sign out of your account when not in use

Disclaimer: Information provided here is based on open source without warranty of any kind.

****

Cycord Support Team
E-mail: cycordsupport.mha@gov.in
Land Line: 011- 26531614, 011-26510245
whatsapp: +917292045198
Website: www.cycord.gov.in

ANNEXURE-6

CERT-IN ADVISORY CIAD-2020-0020

Web Conferencing Security

Original Issue Date: April 15, 2020

Severity Rating: High

Description

The recent COVID-19 pandemic has led organizations, educational institutions and many others to incorporate web conferencing for communication from home.

Web conference is a service which enables users to conduct meetings, conferences, presentations, trainings through the internet over TCP/IP connections without being physically present at one single location. Web conferencing allows real time communication offering streams of data through text messages, voice and video calls.

Fraudsters have found this as an opportunity to conduct unauthorized activities resulting in obtaining of sensitive information of individuals and organization such as employee information, product knowledge, trade secrets etc. It is necessary to protect confidential data from prying eyes.

Few security issues while using web conferencing are:

Attackers joining the meeting if no password to join is required or if they get to know the access code.

Attacker sending malicious links in chat to extract information.

Data shared using third parties might be used by attackers to obtain information.

Vulnerabilities if not patched on time could allow attackers to exploit the target system.

Best practices for using Web Conferencing

Install the web conferencing system through a distinguished vendor which allows encryption of data with SSL/TLS limits, provides intrusion control and allows non-persistent flow of data.

Update the system regularly for any vulnerabilities with the latest software and patches.

Review security and privacy settings to prevent attackers from exploiting the system.

Information about the meeting should be given only to concerned individuals via authorized email. Providing of access codes to join the meeting to participants will lead to restriction of data flow.

Consider using waiting room features: Place participants in a separate virtual room before the meeting and allow the host to admit only people who are supposed to be in the room.

Keep an eye on uninvited guest during the web conference. The meeting may be locked for others to join once all valid participants have joined.The host of the web conference should monitor whether only the intended participants have joined in.

Screen sharing should be limited to the host which will restrict sharing of content by the other participants by mistake.

If you do record a meeting, make sure that you get permission from all participants and give the recording a unique name when you save it.

Participants should be aware of their surroundings. Basic rules such as using headphones, muting the microphone when not speaking, using a blank background during video conferencing should be incorporated.

Give information to others in the meeting on a need to know basis by assigning level of information access to all participants.

Kids who have classes through web conferencing should be advised to use the system in a safe and secure manner. They should be advised to discuss only on the topic mentioned by the teacher and not divulge personal information.

Once the web conference is over, the provider should erase all data from its server.

References

https://www.welivesecurity.com/2020/03/30/work-from-home-videoconferencing-security-in-mind/
https://blog.paloaltonetworks.com/2020/04/network-video-conferencing-security/
https://www.cyber.gov.au/publications/web-conferencing-security
https://sentreesystems.com/newsletter-topics/web-conferencing-security-tips/
https://www.computerworld.com/article/3535924/do-s-and-don-ts-of-videoconferencing-security.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572
Postal address
Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India