CIS Benchmarks

CIS Zoom Benchmark

v1.0.0 - 10-22-2020

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Terms of Use 1
Overview 12
Intended Audience 12
Consensus Guidance 12
Typographical Conventions 13
Assessment Status 13
Profile Definitions 14
Acknowledgements 15
Recommendations 16
1 Account Settings 16
1.1 Meeting 16
1.1.1 Security 16
1.1.1.1.1 Ensure minimum passcode length is set to at least 6 characters (Manual) 17
1.1.1.1.2 Ensure passcode is set to have at least 1 letter (Manual) 18
1.1.1.1.3 Ensure passcode is set to have at least 1 number (Manual) 19
1.1.1.1.4 Ensure passcode is set to have at least 1 special character (Manual) 20
1.1.1.1.5 Ensure passcode include both uppercase and lowercase characters is set to enabled (Manual) 21
1.1.1.1.6 Ensure passcode cannot contain consecutive characters is set to enabled (Manual) 22
1.1.1.1.7 Ensure enhanced weak passcode detection is set to enabled (Manual) . 23
1.1.1.1.8 Ensure only allow numeric passcode is set to disabled (Manual) 24
1.1.1.2 Ensure waiting room is set to enabled (Manual) 25
1.1.1.3 Ensure waiting room options is set to everyone (Manual) 26
1.1.1.4 Ensure require a passcode when scheduling new meetings is set to enabled (Manual) 27
1.1.1.5 Ensure room meeting ID passcode is set to enabled (Manual) 28
1.1.1.6 Ensure require a password for instant meetings is set to enabled (Manual) 29

1.1.1.7 Ensure require a password for Personal Meeting ID (PMI) is set to enabled (Manual) 30
1.1.1.8 Ensure embed password in meeting link for one-click join is set to enabled (Manual) 31
1.1.1.9 Ensure only authenticated users can join meetings is set to enabled (Manual) 32
1.1.1.10 Ensure require password for participants joining by phone is set to enabled (Manual) 33
1.1.1.11 Ensure only authenticated users can join meetings from Web client is set to enabled (Manual) 34
1.1.2 Schedule Meeting 35
1.1.2.1.1 Have a minimum password length (Automated) 36
1.1.2.1.2 Specify a password length: (Automated) 37
1.1.2.1.3 Have at least 1 letter (a, b, c...) (Automated) 38
1.1.2.1.4 Have at least 1 number (1, 2, 3...) (Automated) 39
1.1.2.1.5 Have at least 1 special character (!, @, #...) (Manual) 40
1.1.2.1.6 Include both uppercase and lower case letters (Automated) 41
1.1.2.2 Ensure host video is set to disabled (Manual) 42
1.1.2.3 Ensure participants video is set to disabled (Manual) 43
1.1.2.4 Ensure join before host is set to disabled (Automated) 44
1.1.2.5 Ensure enable personal meeting ID is set to enabled (Manual) 45
1.1.2.6 Ensure use personal meeting ID (PMI) when scheduling a meeting is set to disabled (Manual) 46
1.1.2.7 Ensure use personal meeting ID (PMI) when starting an instant meeting is set to disabled (Manual) 47
1.1.2.8 Ensure add watermark is set to enabled (Manual) 48
1.1.2.9 Ensure add audio watermark is set to enabled (Manual) 49
1.1.2.10 Ensure always display "Zoom Meeting" as the meeting topic is set to enabled (Manual) 50
1.1.2.11 Ensure bypass the password when joining meetings from meeting list is set to enabled (Manual) 51
1.1.2.12 Ensure mute participants upon entry is set to enabled (Manual) 52
1.1.2.13 Ensure upcoming meeting reminder is set to enabled (Manual) 53

1.1.3 In Meeting (Basic) 54
1.1.3.1.1 Ensure allow meeting participants to send a message visible to all participants is set to disabled (Manual) 55
1.1.3.1.2 Ensure prevent participants from saving chat is set to enabled (Manual) 56
1.1.3.2.1 Ensure sound notification when someone joins or leaves is set to enabled (Manual) 57
1.1.3.2.2 Ensure play sound for "Host and co-host only" is set to enabled (Manual) 58
1.1.3.2.3 Ensure when someone joins by phone, ask to record their voice to use as the notification is set to enabled (Manual) 59
1.1.3.3.1 Ensure hosts and participants can send files through the in-meeting chat is set to disabled (Manual) 60
1.1.3.3.2 Ensure only allow specified file types is set to enabled (Manual) 61
1.1.3.4.1 Ensure screen sharing is set to enabled (Manual) 62
1.1.3.4.2 Ensure "who can share?" is set to "Host Only" (Manual) 63
1.1.3.4.3 Ensure "Who can start sharing when someone else is sharing?" is set to "Host Only" (Manual) 64
1.1.3.5.1 Ensure annotation is set to disabled (Manual) 65
1.1.3.5.2 Ensure allow saving of shared screens with annotations is set to disabled (Manual) 66
1.1.3.5.3 Ensure only the user who is sharing can annotate is set to enabled (Manual) 67
1.1.3.6.1 Ensure whiteboard is set to disabled (Manual) 68
1.1.3.6.2 Ensure allow saving of whiteboard content is set to disabled (Manual) 69
1.1.3.6.3 Ensure auto save whiteboard content when sharing is stopped is set to disabled (Manual) 70
1.1.3.7 Ensure require encryption for 3rd party endpoints (SIP/H.323) is set to enabled (Manual) 71
1.1.3.8 Ensure allow meeting participants to send a private 1:1 message to another participant is set to disabled (Manual) 72
1.1.3.9 Ensure auto saving chats is set to enabled (Manual) 73
1.1.3.10 Ensure feedback to Zoom is set to enabled (Manual) 74

1.1.3.11 Ensure co-host is set to enabled (Manual) 75
1.1.3.12 Ensure polling is set to enabled (Manual) 76
1.1.3.13 Ensure always show meeting control toolbar is set to enabled (Manual) 77
1.1.3.14 Ensure show Zoom windows during screen share is set to enabled (Manual) 78
1.1.3.15 Ensure disable desktop/screen share for users is set to enabled (Manual) 79
1.1.3.16 Ensure remote control is set to disabled (Manual) 80
1.1.3.17 Ensure nonverbal feedback is set to disabled (Manual) 81
1.1.3.18 Ensure meeting reactions is set to disabled (Manual) 82
1.1.3.19 Ensure allow removed participants to rejoin is set to disabled (Manual) 83
1.1.3.20 Ensure allow participants to rename themselves is set to enabled (Manual) 84
1.1.3.21 Ensure hide participant profile pictures in a meeting is set to disabled (Manual) 85
1.1.4 In Meeting (Advanced) 86
1.1.4.1.1 Ensure select data center regions for meetings/webinars hosted by your account is set to enabled (Manual) 87
1.1.4.1.2 Ensure data center regions is set to local countries (Manual) 88
1.1.4.2.1 Ensure breakout room is set to enabled (Manual) 89
1.1.4.2.2 Ensure allow host to assign participants to breakout rooms when scheduling is set to enabled (Manual) 90
1.1.4.3.1 Ensure virtual background is set to enabled (Manual) 91
1.1.4.3.2 Ensure allow use of videos for virtual backgrounds is set to disabled (Manual) 92
1.1.4.3.3 Ensure allow users to upload custom backgrounds is set to disabled (Manual) 93
1.1.4.4.1 Ensure peer to peer connection while only 2 people in a meeting is set to disabled (Manual) 94
1.1.4.4.2 Enable listening ports range is set as appropriate for organization (Manual) 95

1.1.4.5 Ensure report participants to Zoom is set to enabled (Manual) 97
1.1.4.6 Ensure remote support is set to disabled (Manual) 98
1.1.4.7 Ensure closed captioning is set to disabled (Manual) 99
1.1.4.8 Ensure save captions is set to disabled (Manual) 100
1.1.4.9 Ensure far end camera control is set to disabled (Manual) 101
1.1.4.10 Ensure identify guest participants in the meeting/webinar is set to enabled (Manual) 102
1.1.4.11 Ensure auto-answer group in chat is set to disabled (Manual) 103
1.1.4.12 Ensure only show default email when sending email invites is set to enabled (Manual) 104
1.1.4.13 Ensure use HTML format email for Outlook plugin is set to enabled (Manual) 105
1.1.4.14 Ensure show a "Join from your browser" link is set to enabled (Manual) 106
1.1.4.15 Ensure allow live streaming meetings is set to disabled (Manual) 107
1.1.4.16 Ensure allow Skype for Business (Lync) client to join a Zoom meeting is set to disabled (Manual) 108
1.1.4.17 Ensure request permission to unmute is set to enabled (Manual) 109
1.1.5 Calendar and Contacts 110
1.1.5.1 Ensure calendar and contacts integration is set to disabled (Manual) 111
1.1.5.2 Ensure ask users to integrate Office 365 calendar when they sign in is set to disabled (Manual) 112
1.1.5.3 Ensure consent to Office 365 calendar integration permissions on behalf of entire account is set to disabled (Manual) 113
1.1.5.4 Ensure enforce OAuth 2.0 for Office 365 calendar integration is set to enabled (Manual) 114
1.1.6 Email Notification 115
1.1.6.1.1 Ensure when a cloud recording is available is set to enabled (Manual) 116
1.1.6.1.2 Ensure Send a copy to the person who scheduled the meeting/webinar for the host is set to enabled (Manual) 117
1.1.6.1.3 Ensure send a copy to the Alternative Hosts is set to enabled (Manual) 118

1.1.6.2 Ensure when attendees join meeting before host is set to enabled (Manual) 119
1.1.6.3 Ensure when a meeting is cancelled is set to enabled (Manual) 120
1.1.6.4 Ensure when an alternative host is set or removed from a meeting is set to enabled (Manual) 121
1.1.6.5 Enable when someone scheduled a meeting for a host is set to enabled (Manual) 122
1.1.6.6 Ensure when the cloud recording is going to be permanently deleted from trash is set to enabled (Manual) 123
1.1.7 Admin Options 124
1.1.7.1 Ensure blur snapshot on iOS task switcher is set to enabled (Manual) 125
1.1.7.2 Ensure display meetings scheduled for others is set to enabled (Manual) 126
1.1.7.3 Ensure use content delivery network (CDN) is set to "Default" (Manual) 127
1.1.7.4 Ensure allow users to contact Zoom's support via chat is set to enabled (Manual) 128
1.2 Recording 129
1.2.1 Local recording 130
1.2.1.1 Ensure local recording is set to enabled (Manual) 130
1.2.1.2 Ensure hosts can give participants the permission to record locally is set to enabled (Manual) 131
1.2.2 Cloud recording 132
1.2.2.1 Ensure cloud recording is set to enabled (Manual) 132
1.2.2.2 Ensure record active speaker with shared screen is set to enabled (Manual) 133
1.2.2.3 Ensure record gallery view with shared screen is set to enabled (Manual) 134
1.2.2.4 Ensure record active speaker, gallery view and shared screen separately is set to enabled (Manual) 135
1.2.2.5 Ensure record an audio only file is set to enabled (Manual) 136
1.2.2.6 Ensure save chat messages from the meeting / webinar is set to enabled (Manual) 137

1.2.3 Advanced cloud recording settings....138
1.2.3.1 Ensure add a timestamp to the recording is set to enabled (Manual)....138
1.2.3.2 Ensure display participants' names in the recording is set to enabled (Manual)....139
1.2.3.3 Ensure record thumbnails when sharing is set to enabled (Manual)....140
1.2.3.4 Ensure optimize the recording for 3rd party video editor is set to enabled (Manual)....141
1.2.3.5 Ensure save panelist chat to the recording is set to enabled (Manual)....142
1.2.4 Automatic recording....143
1.2.4.1 Ensure automatic recording is set to enabled (Manual)....143
1.2.4.2 Ensure automatic recording is set to "Record in the Cloud" (Manual)....144
1.2.4.3 Ensure host can pause/stop the auto recording in the cloud is set to enabled (Manual)....145
1.2.5 Cloud recording downloads....146
1.2.5.1 Ensure cloud recording downloads is set to enabled (Manual)....146
1.2.5.2 Ensure only the host can download cloud recordings is set to enabled (Manual)....147
1.2.6 Set minimum passcode strength requirements....148
1.2.6.1 Ensure have a minimum passcode length is set to 8 characters or greater (Manual)....148
1.2.6.2 Ensure passcode have at least 1 letter is set to enabled (Manual)....149
1.2.6.3 Ensure passcode have at least 1 number is set to enabled (Manual)....150
1.2.6.4 Ensure passcode have at least 1 special character is set to enabled (Manual)....151
1.2.6.5 Ensure allow numeric passcode is set to disabled (Manual)....152
1.2.7 Recording disclaimer....153
1.2.7.1 Ensure recording disclaimer is set to enabled (Manual)....153
1.2.7.2 Ensure ask participants for consent when a recording starts is set to enabled (Manual)....154
1.2.7.3 Ensure ask host to confirm before starting a recording is set to enabled (Manual)....155
1.2.8 Ensure prevent hosts from accessing their cloud recordings is set to enabled (Manual)....156

1.2.9 Ensure IP address access control is set to organization approved ranges (Manual) 157
1.2.10 Ensure require passcode to access shared cloud recordings is set to enabled (Manual) 158
1.2.11 Ensure the host can delete cloud recordings is set to disabled (Manual) 159
1.2.12 Ensure allow recovery of deleted cloud recordings from trash is set to enabled (Manual) 160
1.2.13 Ensure multiple audio notifications of recorded meeting is set to enabled (Manual) 161
1.3 Telephone 162
1.3.1 Ensure toll call is set to enabled (Manual) 163
1.3.2 Ensure mask phone number in the participant list is set to enabled (Manual) 164
1.3.3 Ensure global dial-in countries/regions is set to enabled (Manual) 165
2 IM Management 166
2.1 IM Settings 166
2.1.1 Sharing 167
2.1.1.1 Ensure screen capture is set to disabled (Manual) 167
2.1.1.2 Ensure code snippet is set to disabled (Manual) 168
2.1.1.3 Ensure animated GIF images is set to disabled (Manual) 169
2.1.1.4 Ensure file transfer is set to disabled (Manual) 170
2.1.2 Visibility 171
2.1.2.1 Ensure set chat as a default tab for first-time users is set to disabled (Manual) 171
2.1.2.2 Ensure show H.323 contacts is set to disabled (Manual) 172
2.1.2.3 Ensure company contacts is set to disabled (Manual) 173
2.1.2.4 Ensure IM groups is set to enabled (Manual) 174
2.1.2.5 Ensure announcements is set to disabled (Manual) 175
2.1.3 Security 176
2.1.3.1 Ensure enable advanced chat encryption is set to enabled (Manual) 176
2.1.3.2 Ensure enable personal channel in chat window is set to disabled (Manual) 177

2.1.3.3 Ensure allow users to add contacts is set to disabled (Manual) 178
2.1.3.4 Ensure allow users to chat with others is set to disabled (Manual) 179
2.1.3.5 Ensure show status to external contacts is set to disabled (Manual) 180
2.1.4 Storage 181
2.1.4.1 Ensure cloud storage is set to enabled (Manual) 181
2.1.4.2 Ensure delete local data is set to disabled (Manual) 182
2.1.4.3 Ensure store edited and deleted message revisions is set to disabled (Manual) 183
2.1.4.4 Ensure third party archiving is set to disabled (Manual) 184
2.2 Enable IM groups is set to the organization's needs (Manual) 185
3 Advanced 186
3.1 Security 186
3.1.1 Authentication 186
3.1.1.1.1 Ensure minimum password length is set to 9 characters or greater (Manual) 187
3.1.1.1.2 Ensure password have at least 1 special character is set to enabled (Manual) 188
3.1.1.1.3 Ensure password cannot contain consecutive characters is set to enabled (Manual) 189
3.1.1.1.4 Ensure use enhanced weak password detection is set to enabled (Manual) 190
3.1.1.2.1 Ensure new users need to change their passwords upon first sign-in is set to enabled (Manual) 191
3.1.1.2.2 Ensure password expires automatically and needs to be changed after 365 days (Manual) 192
3.1.1.2.3 Ensure users cannot reuse any password used in the last 5 times or more (Manual) 193
3.1.1.2.4 Enable users can change their password 1 time every 24 hours (Manual) 194
3.1.1.3.1 Ensure only account admin can change licensed users' personal meeting ID and personal link name (Manual) 195
3.1.1.3.2 Ensure allow importing of photos from the photo library on the user's device is set to disabled (Manual) 196

3.1.1.3.3 Ensure hide billing information from administrators is set to enabled (Manual) 197
3.2 Ensure integration is set to appropriate organizational needs (Manual) 198
Appendix: Summary Table 199
Appendix: Change History 207

Overview

This document, CIS Zoom Benchmark, provides prescriptive guidance for establishing a secure configuration posture for Zoom. This guide was tested against Zoom videoconferencing software. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Zoom Video Communication.

Consensus Guidance

This benchmark was created using a consensus review process comprised of subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as a defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor
Darren Freidel, Center for Internet Security
Todd Lamothe Microsoft MVP Reconnect, MSCE, MCSA, MCT, Nattrac Consulting Ltd.
Phil White , Center for Internet Security

Editor
Vittal Sher COBITv5F, CISA, CIPR, ITILv3, MCSE, CCNA, CDPSE

Recommendations

1 Account Settings

1.1 Meeting

Where you can set settings for meetings for the organization.

Groups and members will use the following settings by default. If you don't want the settings below to be changed, you can lock the settings here

1.1.1 Security

1.1.1.1 Passcode Requirement

1.1.1.1.1 Ensure minimum passcode length is set to at least 6 characters (Manual)

Profile Applicability:

- Level 1

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. Minimum passcode length must be at least 6 characters.

Rationale:

This ensures the passcode complexity requirements are met and a strong passcode is set for meetings.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have a minimum passcode length, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have a minimum passcode length, and ensure it is set to enabled.

Default Value:

Unchecked

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.2 Ensure passcode is set to have at least 1 letter (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. As per passcode requirements, have at least 1 letter (a, b, c...). This shall make the passcode strong.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have at least 1 letter (a, b, c...), and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have at least 1 letter (a, b, c...), and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.3 Ensure passcode is set to have at least 1 number (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. As per passcode requirements, Have at least 1 number (1, 2, 3...). This shall make the passcode strong.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have at least 1 number (1, 2, 3...), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have at least 1 number (1, 2, 3...), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.4 Ensure passcode is set to have at least 1 special character (Manual)

Profile Applicability:

- Level 2

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. As per passcode requirements, Have at least 1 special character (!, @, #...). This shall make the passcode strong.

Rationale:

This ensures the passcode complexity requirements are met and a strong passcode is set for meetings.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have at least 1 special character (!, @, #...), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Have at least 1 special character (!, @, #...), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.5 Ensure passcode include both uppercase and lowercase characters is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. As per passcode requirements, Include both uppercase and lowercase characters. This shall make the passcode strong.

Rationale:

This ensures the passcode complexity requirements are met and a strong passcode is set for meetings.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Include both uppercase and lowercase characters, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Include both uppercase and lowercase characters, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.6 Ensure passcode cannot contain consecutive characters is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. Cannot contain consecutive characters (e.g. “11111”, “12345”, “abcde”, or “qwert”).

Rationale:

This ensures the passcode complexity requirements are met and a strong passcode is set for meetings.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Cannot contain consecutive characters (e.g. “11111”, “12345”, “abcde”, or “qwert”), and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Cannot contain consecutive characters (e.g. “11111”, “12345”, “abcde”, or “qwert”), and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.7 Ensure enhanced weak passcode detection is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

For security purposes, Zoom has a few requirements that your passcode can meet. As per passcode requirements, Use enhanced weak passcode detection. This shall make the passcode strong.

Rationale:

This ensures the passcode complexity requirements are met and a strong passcode is set for meetings.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Use enhanced weak passcode detection, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Use enhanced weak passcode detection, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.1.8 Ensure only allow numeric passcode is set to disabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

For security purposes, Zoom has a few requirements that your passcode must meet. As per passcode requirements, Disable “Only allow numeric passcode”, enabling this shall make the passcode weaker.

Rationale:

This ensures the passcode complexity requirements are met and a strong passcode is set for meetings.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Only allow numeric passcode, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Passcode Requirement -> Only allow numeric passcode, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.2 Ensure waiting room is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Rationale:

This option ensures that the participants are by default entered into meeting.

Impact:

When hundreds of participants are joining, the Co-Hosts has to admit all participants and may take time.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Waiting Room and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Waiting Room and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.3 Ensure waiting room options is set to everyone (Manual)

Profile Applicability:

- Level 1

Description:

Click on "Edit Options" to choose who should go in the waiting room? A) Everyone, B) Users not in your account, C) Users who are not in your account and not part of the allowed domains

Rationale:

This shall increase the security by choosing which participants should go into waiting room when joining a meeting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Security -> Waiting Room Option and click on “Edit Options” to see which option is selected.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Security -> Waiting Room Option and click on “Edit Options” to and ensure “Everyone” option is selected.

References:

1. https://support.zoom.us/hc/en-us/articles/115000332726-Waiting-Room

Additional Information:

See the reference zoom link to customize waiting room features.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.4 Ensure require a passcode when scheduling new meetings is set to enabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Require a passcode when scheduling new meetings must be set to enabled. A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting.

Rationale:

Upon scheduling a meeting, a passcode will be generated, this ensures that participants require the passcode to join the meeting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require a passcode when scheduling new meetings and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require a passcode when scheduling new meetings and ensure it is set to enabled.

References:

1. https://support.zoom.us/hc/en-us/articles/115005756143

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.5 Ensure room meeting ID passcode is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

All Room Meeting ID meetings that users can join via client, phone, or room systems will be passcode-protected.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Room Meeting ID Passcode, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Room Meeting ID Passcode, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.6 Ensure require a password for instant meetings is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

A random passcode will be generated when starting an instant meeting.

Rationale:

Enabling this setting shall increase security for meetings that are created instantly. A participant requires the passcode to be entered for joining.

Impact:

This setting may not be helpful in a scenario, where participants need to join a meeting that was created instantly and does not want to input a passcode to join.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require a passcode for instant meetings, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require a passcode for instant meetings, and ensure it is set to enabled.

References:

1. https://support.zoom.us/hc/en-us/articles/115005756143

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.7 Ensure require a password for Personal Meeting ID (PMI) is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Enable "Require a passcode for Personal Meeting ID (PMI)" to set a passcode for meetings that use the personal meeting ID (PMI) and then choose "All meetings using PMI"

Rationale:

This increases security, and ensures that all meetings that are created using PMI requires a passcode to login.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require a passcode for Personal Meeting ID (PMI), and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require a passcode for Personal Meeting ID (PMI), and ensure it is set to enabled. After enabling, check if option “All meetings using PMI” is chosen.

References:

1. https://support.zoom.us/hc/en-us/articles/115005756143

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.8 Ensure embed password in meeting link for one-click join is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

Rationale:

Increased security to avoid need to punch in passcode. When participant clicks on meeting link that was sent to registered email, users joins meeting automatically.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Embed passcode in invite link for one-click join, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Embed passcode in invite link for one-click join, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.9 Ensure only authenticated users can join meetings is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Rationale:

The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Security -> Only authenticated users can join meetings and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Security -> Only authenticated users can join meetings and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.10 Ensure require password for participants joining by phone is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require passcode for participants joining by phone, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Security -> Require passcode for participants joining by phone, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.1.11 Ensure only authenticated users can join meetings from Web client is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Only authenticated users can join meetings from Web client should be set to enabled. This requires users to authenticate and identify themselves prior to logging in and joining a meeting.

Rationale:

Only authenticated users can join meetings from Web client. Users will be known and not anonymous meaning anyone can join.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting ->Only authenticated users can join meetings from Web client and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting ->Only authenticated users can join meetings from Web client and ensure it is set to enabled.

References:

1. https://support.zoom.us/hc/en-us/articles/115005756143

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2 Schedule Meeting

1.1.2.1 Meeting password requirement

1.1.2.1.1 Have a minimum password length (Automated)

Profile Applicability:

- Level 1

Description:

For security purposes, Zoom has a few requirements that your password must meet. These apply when setting your initial password and when resetting your password. Minimum password length must be at least 8 characters.

Rationale:

This ensures the password complexity requirements are met and a strong password is set for the account.

Audit:

Remediation:

Default Value:

Must be at least 8 characters

References:

1. https://support.zoom.us/hc/en-us/articles/115005166483-Managing-your-password

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.1.2 Specify a password length: (Automated)

Profile Applicability:

- Level 1

Description:

For security purposes, Zoom has a few requirements that your password must meet. These apply when setting your initial password and when resetting your password. Password length must be at least 8 characters and cannot be longer than 32 characters.

Rationale:

Audit:

Remediation:

References:

1. https://support.zoom.us/hc/en-us/articles/115005166483-Managing-your-password

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.1.3 Have at least 1 letter (a, b, c...) (Automated)

Profile Applicability:

- Level 1

Description:

For security purposes, Zoom has a few requirements that your password must meet. These apply when setting your initial password and when resetting your password. As per password requirements, have at least 1 letter (a, b, c...). This shall make the password strong.

Rationale:

Audit:

Remediation:

References:

1. https://support.zoom.us/hc/en-us/articles/115005166483-Managing-your-password

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.1.4 Have at least 1 number (1, 2, 3...) (Automated)

Profile Applicability:

- Level 1

Description:

For security purposes, Zoom has a few requirements that your password must meet. These apply when setting your initial password and when resetting your password. As per password requirements, have at least 1 number (1, 2, 3...). This shall make the password strong.

Rationale:

Audit:

Remediation:

References:

1. https://support.zoom.us/hc/en-us/articles/115005166483-Managing-your-password

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.1.5 Have at least 1 special character (!, @, #...) (Manual)

Profile Applicability:

- Level 2

Description:

For security purposes, Zoom has a few requirements that your password must meet. These apply when setting your initial password and when resetting your password. As per password requirements, include at least 1 special character (!, @, #...).

Rationale:

Audit:

Remediation:

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.1.6 Include both uppercase and lower case letters (Automated)

Profile Applicability:

- Level 2

Description:

For security purposes, Zoom has a few requirements that your password must meet. These apply when setting your initial password and when resetting your password. As per password requirements, include both uppercase and lower case letters.

Rationale:

Audit:

Remediation:

References:

1. https://support.zoom.us/hc/en-us/articles/115005166483-Managing-your-password

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.2 Ensure host video is set to disabled (Manual)

Profile Applicability:

- Level 1

Description:

Start meetings with host video on should be set to disabled.

Rationale:

Enforcing a Zoom default setting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Host video, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Host video, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.3 Ensure participants video is set to disabled (Manual)

Profile Applicability:

- Level 1

Description:

Start meetings with Participants video on should be set to disabled and locked off.

Rationale:

This ensures people joining a meeting do not have their camera on without them realizing. Locking the setting ensures no one changes this when creating a meeting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Participants video, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Participants video, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.4 Ensure join before host is set to disabled (Automated)

Profile Applicability:

- Level 1

Description:

Allow participants to join the meeting before the host arrives should be set to disabled and locked off.

Rationale:

This ensures people joining a meeting do not enter a meeting before the host has arrived. If there are annoying users, they cannot be removed or muted until the host arrives. Locking the setting ensures no one changes this when creating a meeting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Join before host, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Join before host, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.5 Ensure enable personal meeting ID is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

A Personal Meeting ID (PMI) is a dedicated 9-11 digit number which is assigned to each individuals account. This becomes the users personal meeting room. This is the personal room assigned upon account creation.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Enable Personal Meeting ID, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Enable Personal Meeting ID, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.6 Ensure use personal meeting ID (PMI) when scheduling a meeting is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Use Personal Meeting ID (PMI) when scheduling a meeting should be set to disabled.

Rationale:

This ensures a new meeting ID is used for new scheduled meetings. If there are nuisance users, they cannot be use an old meeting ID to join a meeting.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Use Personal Meeting ID (PMI) when scheduling a meeting, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Use Personal Meeting ID (PMI) when scheduling a meeting, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.7 Ensure use personal meeting ID (PMI) when starting an instant meeting is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Use Personal Meeting ID (PMI) when starting an instant meeting should be set to disabled.

Rationale:

Use Personal Meeting ID (PMI) when starting an instant meeting set to disabled ensures that someone who knows a personal meeting ID from a previous meeting cannot join a meeting without a proper invitation and knowing the code.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Use Personal Meeting ID (PMI) when starting an instant meeting, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Use Personal Meeting ID (PMI) when starting an instant meeting, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.8 Ensure add watermark is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Adding watermark enables author accreditation. Each attendee sees a portion of their own email address embedded as a watermark in any shared content and on the video of the participant who is sharing their screen. This option requires enabling "Only signed-in users can join the meeting" or "Only signed-in users with specified domains can join meetings".

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Add watermark, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Add watermark, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.9 Ensure add audio watermark is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Adding audio watermark, enables invisible accreditation. If an attendee records the meeting, their personal information will be embedded in the audio as an inaudible watermark. This option requires enabling "Only signed-in users can join the meeting" or "Only signed-in users with specified domains can join meetings".

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Add audio watermark, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Scheduled Meeting -> Add audio watermark, and check if it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.10 Ensure always display "Zoom Meeting" as the meeting topic is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Hide actual meeting topic and display "Zoom Meeting" for your scheduled meetings. Helps confidentiality of meeting topic public display.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Schedule Meeting -> Always display "Zoom Meeting" as the meeting topic, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Schedule Meeting -> Always display "Zoom Meeting" as the meeting topic, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.11 Ensure bypass the password when joining meetings from meeting list is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

When Zoom Rooms join a scheduled meeting on its meeting list, users do not need to manually enter the meeting passcode.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Schedule Meeting -> Bypass the passcode when joining meetings from meeting list, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Schedule Meeting -> Bypass the passcode when joining meetings from meeting list, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.12 Ensure mute participants upon entry is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves, through client end by enabling "Allow Participants to Unmute Themselves" under more options in participants list.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Schedule Meeting -> Mute participants upon entry, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Schedule Meeting -> Mute participants upon entry, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.2.13 Ensure upcoming meeting reminder is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable this option to receive desktop notification for upcoming meetings. Reminder time can be configured in the Zoom Desktop Client.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Settings -> Meeting -> Schedule Meeting -> Upcoming meeting reminder and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Settings -> Meeting -> Schedule Meeting -> Upcoming meeting reminder and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3 In Meeting (Basic)

1.1.3.1 Chat

1.1.3.1.1 Ensure allow meeting participants to send a message visible to all participants is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow meeting participants to send a message visible to all participants. This can be further controlled from client end by the host / co-host.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow meeting participants to send a message visible to all participants, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow meeting participants to send a message visible to all participants, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.1.2 Ensure prevent participants from saving chat is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Prevent participants from saving chat, ensures that participants do not copy what is pasted in the zoom meeting chat.

Rationale:

Impact:

Disables the ability of participants from copying content from chat, which may have been purposefully shared by the host to participants.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Prevent participants from saving chat, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Prevent participants from saving chat, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.2 Sound notification when someone joins or leaves

1.1.3.2.1 Ensure sound notification when someone joins or leaves is set to enabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Enable "Play sound when participants join or leave". This can also be controlled from host client end if required to be changed.

Rationale:

This option enables Host and co-hosts to know that participants are joining/leaving.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Sound notification when someone joins or leaves, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Sound notification when someone joins or leaves, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.2.2 Ensure play sound for "Host and co-host only" is set to enabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Change from "Everyone" option under [Play sound for] to "Host and co-hosts only".

Rationale:

This option enables Host and co-hosts to know that participants are joining/leaving.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Sound notification when someone joins or leaves -> Play sound for -> Host and co-hosts only, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Sound notification when someone joins or leaves -> Play sound for -> Host and co-hosts only, and check ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.2.3 Ensure when someone joins by phone, ask to record their voice to use as the notification is set to enabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Select "Ask to record their voice to use as the notification" option for "When someone joins by phone".

Rationale:

This option enables Host and co-hosts to know that participants are joining/leaving while joining from phone.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Sound notification when someone joins or leaves -> When someone joins by phone -> Ask to record their voice to use as the notification, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Sound notification when someone joins or leaves -> When someone joins by phone -> Ask to record their voice to use as the notification, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.3 File transfer

1.1.3.3.1 Ensure hosts and participants can send files through the in-meeting chat is set to disabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Hosts and participants can send files through the in-meeting chat. As this is account level setting keep this enabled. If option of file transfer is required, then use it along with allowing specific file extension.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Hosts and participants can send files through the in-meeting chat., and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Hosts and participants can send files through the in-meeting chat., and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.3.2 Ensure only allow specified file types is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Hosts and participants can send files through the in-meeting chat. And that too only the file types that are whitelisted. Provide the list of filetype that needs to be whitelisted e.g. .txt, .docx, .pdf, .xlsx

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Only allow specified file types, and check if it is enabled (i.e. checkbox enabled).

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Only allow specified file types, and ensure it is enabled (i.e. checkbox enabled).

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.4 Screen sharing

1.1.3.4.1 Ensure screen sharing is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Allow host and participants to share their screen or content during meetings. Enable this option to ensure further options are customizable to control who can share screen or desktop audio.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Screen sharing, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Screen sharing, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.4.2 Ensure "who can share?" is set to "Host Only" (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Select "Who can share?" as "Host Only" here. This can be controlled by host for a particular meeting at desktop client software.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Who can share?, and check if “Host Only” is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Who can share?, and ensure “Host Only” is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.4.3 Ensure "Who can start sharing when someone else is sharing?" is set to "Host Only" (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

This setting decides who can share screen when someone is already sharing. This option should be restricted to "Host Only". This can be changed or controlled by host for a particular meeting instance.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Who can start sharing when someone else is sharing? and check if “Host Only” is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Who can start sharing when someone else is sharing? and ensure “Host Only” is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.5 Annotation

1.1.3.5.1 Ensure annotation is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host and participants to use annotation tools to add information to shared screens.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Annotation and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Annotation and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.5.2 Ensure allow saving of shared screens with annotations is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Disable "Allow saving of shared screens with annotations"

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow saving of shared screens with annotations and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow saving of shared screens with annotations and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.5.3 Ensure only the user who is sharing can annotate is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable "Only the user who is sharing can annotate", to ensure that only host can annotate.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Only the user who is sharing can annotate and check if it is enabled (i.e, checkbox enabled).

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Only the user who is sharing can annotate and ensure it is enabled (i.e, checkbox enabled).

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.6 Whiteboard

1.1.3.6.1 Ensure whiteboard is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host and participants to share whiteboard during a meeting.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Whiteboard and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Whiteboard and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.6.2 Ensure allow saving of whiteboard content is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host and participants to share whiteboard during a meeting. And also allow saving of whiteboard content. This can be controlled at meeting level.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow saving of whiteboard content and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow saving of whiteboard content and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.6.3 Ensure auto save whiteboard content when sharing is stopped is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host and participants to share whiteboard during a meeting. And disallow Auto save whiteboard content when sharing is stopped. This can be controlled at meeting level.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Auto save whiteboard content when sharing is stopped and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Auto save whiteboard content when sharing is stopped and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.7 Ensure require encryption for 3rd party endpoints (SIP/H.323) is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

By default, Zoom requires encryption for all data transferred between the Zoom cloud, Zoom client, and Zoom Room. Turn on this setting to require encryption for 3rd party endpoints (SIP/H.323) as well.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Require encryption for 3rd party endpoints (SIP/H.323) and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Require encryption for 3rd party endpoints (SIP/H.323) and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.8 Ensure allow meeting participants to send a private 1:1 message to another participant is set to disabled (Manual)

Profile Applicability:

- Level 1

Description:

Allow meeting participants to send a private 1:1 message to another participant.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow meeting participants to send a private 1:1 message to another participant., and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow meeting participants to send a private 1:1 message to another participant., and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.9 Ensure auto saving chats is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Auto saving chats, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Auto saving chats, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.10 Ensure feedback to Zoom is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Add a Feedback tab to the Windows Settings or Mac Preferences dialog, and also enable users to provide feedback to Zoom at the end of the meeting.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Feedback to Zoom, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Feedback to Zoom, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.11 Ensure co-host is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Co-host, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Co-host, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.12 Ensure polling is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Add 'Polls' to the meeting controls. This allows the host to survey the attendees. Polls also enables the host to validate if participants are active.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Polling, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Polling, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.13 Ensure always show meeting control toolbar is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Always show meeting controls during a meeting. This helps in responding to situations where host / co-host need to quickly navigate controls to handle a situation.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Always show meeting control toolbar, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Always show meeting control toolbar, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.14 Ensure show Zoom windows during screen share is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Show Zoom windows during screen share. This shall help in quickly controlling a situation where someone needs to be muted/removed from the meeting.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Show Zoom windows during screen share, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Show Zoom windows during screen share, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.15 Ensure disable desktop/screen share for users is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Disable desktop or screen share in a meeting and only allow sharing of selected applications.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Disable desktop/screen share for users, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Disable desktop/screen share for users, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.16 Ensure remote control is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

During screen sharing, the person who is sharing can allow others to control the shared content.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Remote control, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Remote control, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.17 Ensure nonverbal feedback is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Participants in a meeting can provide nonverbal feedback and express opinions by clicking on icons in the Participants panel. Disabling this avoids participants misusing this feature.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Nonverbal feedback, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Nonverbal feedback, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.18 Ensure meeting reactions is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow meeting participants to communicate without interrupting by reacting with an emoji that shows on their video. Reactions disappear after 10 seconds. Participants can change their reaction skin tone in Settings. This option can be misused by mischievous participants.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Meeting reactions, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Meeting reactions, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.19 Ensure allow removed participants to rejoin is set to disabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Allows previously removed meeting participants and webinar panelists to rejoin. If this option is enabled, then any distracting participants that were removed will be able to join back again.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow removed participants to rejoin, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow removed participants to rejoin, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.20 Ensure allow participants to rename themselves is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Allow meeting participants and webinar panelists to rename themselves. This option is required to identify participants in a meeting that does not require registration. Also, this options helps participants to rename themselves to self-identify.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow participants to rename themselves, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Allow participants to rename themselves, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.3.21 Ensure hide participant profile pictures in a meeting is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

All participant profile pictures will be hidden and only the names of participants will be displayed on the video screen. Participants will not be able to update their profile pictures in the meeting.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Hide participant profile pictures in a meeting, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Basic) -> Hide participant profile pictures in a meeting, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4 In Meeting (Advanced)

1.1.4.1 Select data center regions for meetings/webinars hosted by your account

1.1.4.1.1 Ensure select data center regions for meetings/webinars hosted by your account is set to enabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Include all data center regions to provide the best experience for participants joining from all regions. Opting out of data center regions may limit CRC, Dial-in, Call Me, and Invite by Phone options for participants joining from those regions.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Select data center regions for meetings/webinars hosted by your account, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Select data center regions for meetings/webinars hosted by your account, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.1.2 Ensure data center regions is set to local countries (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Not all data centers are configured. Only the required ones are configured. Choose local or trusted region data centers.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Select data center regions for meetings/webinars hosted by your account, and check if local countries are selected. E.g. For United States, select United States.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Select data center regions for meetings/webinars hosted by your account, and ensures local countries are selected. E.g. For United States, select United States.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.2 Breakout room

Breakout rooms allow you to split your Zoom meeting in up to 50 separate sessions. The meeting host can choose to split the participants of the meeting into these separate sessions automatically or manually, and can switch between sessions at any time.

1.1.4.2.1 Ensure breakout room is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host to split meeting participants into separate, smaller rooms. This is beneficial, when participants need to be moved to separate virtual rooms.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Breakout room, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Breakout room, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.2.2 Ensure allow host to assign participants to breakout rooms when scheduling is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host to assign participants to breakout rooms when scheduling.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow host to assign participants to breakout rooms when scheduling, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow host to assign participants to breakout rooms when scheduling, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.3 Virtual background

The Virtual Background feature allows you to display an image or video as your background during a Zoom Meeting.

1.1.4.3.1 Ensure virtual background is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Customize your background to keep your environment private from others in a meeting. This can be used with or without a green screen.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Virtual background, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Virtual background, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.3.2 Ensure allow use of videos for virtual backgrounds is set to disabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Customize your background to keep your environment private from others in a meeting. This can be used with or without a green screen. Allow use of videos for virtual backgrounds.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow use of videos for virtual backgrounds, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow use of videos for virtual backgrounds, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.3.3 Ensure allow users to upload custom backgrounds is set to disabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Customize your background to keep your environment private from others in a meeting. This can be used with or without a green screen. Allow users to upload custom backgrounds. Disabling this option ensures that participants do not have inappropriate backgrounds.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow users to upload custom backgrounds, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow users to upload custom backgrounds, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.4 Peer to Peer connection while only 2 people in a meeting

1.1.4.4.1 Ensure peer to peer connection while only 2 people in a meeting is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to directly connect to one another in a 2-person meeting.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow users to directly connect to one another in a 2-person meeting, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow users to directly connect to one another in a 2-person meeting, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.4.2 Enable listening ports range is set as appropriate for organization (Manual)

Profile Applicability:

- Level 2

Description:

Listening ports range, select the appropriate ports as per your company or organization settings.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Peer to Peer connection while only 2 people in a meeting -> Listening ports range, and check if it is enabled, also appropriate ports are selected as per organization.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Peer to Peer connection while only 2 people in a meeting -> Listening ports range, and ensure it is enabled, also appropriate ports are selected as per organization.

References:

1. https://support.zoom.us/hc/en-us/articles/201362683-Network-firewall-or-proxy-server-settings-for-Zoom

Additional Information:

Use the provided reference to know what all ports Zoom works on.

CIS Controls:

Version 7

12.4 Deny Communication over Unauthorized Ports

Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.

1.1.4.5 Ensure report participants to Zoom is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Hosts can report meeting participants for inappropriate behavior to Zoom's Trust and Safety team for review. This setting can be found on the Security icon on the meeting controls toolbar.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Report participants to Zoom, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Report participants to Zoom, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.6 Ensure remote support is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow meeting host to provide 1:1 remote support to another participant. Do not enable these options unless, you really need them.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Remote support, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Remote support, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.7 Ensure closed captioning is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow host to type closed captions or assign a participant/third party device to add closed captions.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Closed captioning, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Closed captioning, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.8 Ensure save captions is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow participants to save fully closed captions or transcripts.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Save Captions, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Save Captions, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.9 Ensure far end camera control is set to disabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Allow another user to take control of your camera during a meeting. Both users (the one requesting control and the one giving control) must have this option turned on.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Far end camera control, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Far end camera control, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.10 Ensure identify guest participants in the meeting/webinar is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

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.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Identify guest participants in the meeting/webinar, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Identify guest participants in the meeting/webinar, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.11 Ensure auto-answer group in chat is set to disabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Enable users to see and add contacts to 'auto-answer group' in the contact list on chat. Any call from members of this group will be automatically answered.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Auto-answer group in chat, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Auto-answer group in chat, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.12 Ensure only show default email when sending email invites is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to invite participants by email only by using the default email program selected on their computer.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Only show default email when sending email invites, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Only show default email when sending email invites, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.13 Ensure use HTML format email for Outlook plugin is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Use HTML formatting instead of plain text for meeting invitations scheduled with the Outlook plugin.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Use HTML format email for Outlook plugin, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Use HTML format email for Outlook plugin, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.14 Ensure show a "Join from your browser" link is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

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.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Show a "Join from your browser" link, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Show a "Join from your browser" link, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.15 Ensure allow live streaming meetings is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow live streaming meetings. Select Facebook Or Workplace by Facebook Or Youtube Or Custom Live Streaming Service.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow live streaming meetings, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow live streaming meetings, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.16 Ensure allow Skype for Business (Lync) client to join a Zoom meeting is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow internal or external Skype for Business (Lync) client to connect to a Zoom meeting.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow Skype for Business (Lync) client to join a Zoom meeting, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Allow Skype for Business (Lync) client to join a Zoom meeting, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.4.17 Ensure request permission to unmute is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Select this option in the scheduler to request permission to unmute meeting participants and webinar panelists. Permissions, once given, will apply in all meetings scheduled by the same person.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Request permission to unmute, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> In Meeting (Advanced) -> Request permission to unmute, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.5 Calendar and Contacts

1.1.5.1 Ensure calendar and contacts integration is set to disabled (Manual)

Profile Applicability:

- Level 1

Description:

Allow users to integrate calendar and contacts services (Google, Exchange, Office 365) with Zoom. Enabling this option shall invite privacy issues, hence keep this disabled.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Calendar and contacts integration, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Calendar and contacts integration, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.5.2 Ensure ask users to integrate Office 365 calendar when they sign in is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Upon login, users will be asked for calendar access. Enabling this option invites privacy issues, hence it is best to keep it disabled.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Ask users to integrate Office 365 calendar when they sign in, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Ask users to integrate Office 365 calendar when they sign in, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.5.3 Ensure consent to Office 365 calendar integration permissions on behalf of entire account is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

When turned off, the Office 365 administrator will need to consent to calendar integrations on behalf of the account. As an administrator, please choose the same settings configured in Office 365. View the settings on Office 365.

Rationale:

Impact:

By disabling this option, O365 integration will not work.

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Consent to Office 365 calendar integration permissions on behalf of entire account, and check if it is set to disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Consent to Office 365 calendar integration permissions on behalf of entire account, and ensure it is set to disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.5.4 Ensure enforce OAuth 2.0 for Office 365 calendar integration is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

When turned on, calendar services will be authenticated with protocol OAuth 2.0.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Enforce OAuth 2.0 for Office 365 calendar integration, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Calendar and Contacts -> Enforce OAuth 2.0 for Office 365 calendar integration, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6 Email Notification

1.1.6.1 When a cloud recording is available

1.1.6.1.1 Ensure when a cloud recording is available is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Notify host when cloud recording is available. This can enable hosts to validate the recording for any confidential data, prior sharing the video at large.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When a cloud recording is available, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When a cloud recording is available, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.1.2 Ensure Send a copy to the person who scheduled the meeting/webinar for the host is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Send a copy to the person who scheduled the meeting/webinar for the host. This can enable meeting scheduler to validate the recording for any confidential data prior sharing the video at large.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> Send a copy to the person who scheduled the meeting/webinar for the host, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> Send a copy to the person who scheduled the meeting/webinar for the host, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.1.3 Ensure send a copy to the Alternative Hosts is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Send a copy to the Alternative Hosts. This can enable alternate hosts to validate the recording for any confidential data prior sharing the video at large.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> Send a copy to the Alternative Hosts, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> Send a copy to the Alternative Hosts, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.2 Ensure when attendees join meeting before host is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Notify host when participants join the meeting before them

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> Notify host when participants join the meeting before them, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> Notify host when participants join the meeting before them, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.3 Ensure when a meeting is cancelled is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Notify host and participants when the meeting is cancelled.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When a meeting is cancelled, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When a meeting is cancelled, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.4 Ensure when an alternative host is set or removed from a meeting is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

When an alternative host is set or removed from a meeting, Notify the alternative host who is set or removed. Helpful for any investigation.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When an alternative host is set or removed from a meeting, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When an alternative host is set or removed from a meeting, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.5 Enable when someone scheduled a meeting for a host is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

When someone scheduled a meeting for a host, Notify the host there is a meeting is scheduled, rescheduled, or cancelled. Helpful in monitoring the schedule by someone who has permissions to schedule a meeting on behalf of host.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When someone scheduled a meeting for a host, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When someone scheduled a meeting for a host, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.6.6 Ensure when the cloud recording is going to be permanently deleted from trash is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

When the cloud recording is going to be permanently deleted from trash, Notify the host 7 days before the cloud recording is permanently deleted from trash. This is helpful when there are needs to preserve the recordings as per the applicable data retention guidelines.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When the cloud recording is going to be permanently deleted from trash, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Email Notification -> When the cloud recording is going to be permanently deleted from trash, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.7 Admin Options

1.1.7.1 Ensure blur snapshot on iOS task switcher is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot display as the preview screen in the iOS tasks switcher when multiple apps are open.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Blur snapshot on iOS task switcher, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Blur snapshot on iOS task switcher, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.7.2 Ensure display meetings scheduled for others is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Display meetings scheduled for others. If disabled, users will only see their meetings even if they have schedule-for privilege for others.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Display meetings scheduled for others, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Display meetings scheduled for others, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.7.3 Ensure use content delivery network (CDN) is set to "Default" (Manual)

Profile Applicability:

- Level 2

Description:

Allow connections to different CDNs for a better web browsing experience. All users under your organization will use the selected CDN to access static resources. By default, all users use Amazon CloudFront except users in China. Users in China use Wangsu (China) instead.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Use content delivery network (CDN), and check if it is set to enabled and "Default" option is selected.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Use content delivery network (CDN), and ensure it is set to enabled and "Default" option is selected.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.1.7.4 Ensure allow users to contact Zoom's support via chat is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Show Zoom Help badge on the bottom right of the page

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Allow users to contact Zoom's Support via Chat, and check if it is set to enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Meeting -> Admin Options -> Allow users to contact Zoom's Support via Chat, and ensure it is set to enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2 Recording

Configure recording option in Zoom

1.2.1 Local recording

1.2.1.1 Ensure local recording is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow hosts and participants to record the meeting to a local file

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Local recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Local recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.1.2 Ensure hosts can give participants the permission to record locally is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable "Hosts can give participants the permission to record locally"

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Hosts can give participants the permission to record locally, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Hosts can give participants the permission to record locally, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2 Cloud recording

1.2.2.1 Ensure cloud recording is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Allow hosts to record and save the meeting / webinar in the cloud.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2.2 Ensure record active speaker with shared screen is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record active speaker with shared screen

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record active speaker with shared screen, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record active speaker with shared screen, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2.3 Ensure record gallery view with shared screen is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record gallery view with shared screen

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record gallery view with shared screen, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record gallery view with shared screen, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2.4 Ensure record active speaker, gallery view and shared screen separately is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record active speaker, gallery view and shared screen separately. Useful to identify the participants, from various views at a later point in time for audit purpose.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record active speaker, gallery view and shared screen separately, and check if it is enabled and sub-options are checked.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record active speaker, gallery view and shared screen separately, and ensure it is enabled and sub-options are checked.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2.5 Ensure record an audio only file is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record an audio only file. Useful in case of evidence for untampered audio file.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record an audio only file, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Record an audio only file, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.2.6 Ensure save chat messages from the meeting / webinar is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Save chat messages from the meeting / webinar. Useful for any investigations.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Save chat messages from the meeting / webinar, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording -> Save chat messages from the meeting / webinar, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.3 Advanced cloud recording settings

1.2.3.1 Ensure add a timestamp to the recording is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Add a timestamp to the recording by enabling this option.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Add a timestamp to the recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Add a timestamp to the recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.3.2 Ensure display participants' names in the recording is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

This option display participants' names in the recording

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Display participants' names in the recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Display participants' names in the recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.3.3 Ensure record thumbnails when sharing is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record thumbnails when sharing

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Record thumbnails when sharing, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Record thumbnails when sharing, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.3.4 Ensure optimize the recording for 3rd party video editor is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Optimize the recording for 3rd party video editor

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Optimize the recording for 3rd party video editor, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Optimize the recording for 3rd party video editor, and check if it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.3.5 Ensure save panelist chat to the recording is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Save panelist chat to the recording helps as chat audit

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Save panelist chat to the recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Advanced cloud recording settings -> Save panelist chat to the recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.4 Automatic recording

1.2.4.1 Ensure automatic recording is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record meetings automatically as they start. Allows to capture evidence if any incidents that happen at start of meetings.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Automatic recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Automatic recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.4.2 Ensure automatic recording is set to "Record in the Cloud" (Manual)

Profile Applicability:

- Level 2

Description:

Record meetings automatically as they start. This option allows to capture evidence if any incidents that happen at start of meetings. Now select "Record in the cloud" to preserve evidences.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Automatic recording -> Record in the cloud, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Automatic recording -> Record in the cloud, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.4.3 Ensure host can pause/stop the auto recording in the cloud is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Record meetings automatically as they start. This option allows to capture evidence if any incidents that happen at start of meetings. Now select "Host can pause/stop the auto recording in the cloud" to give control to host / co-hosts.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Automatic recording -> Host can pause/stop the auto recording in the cloud, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Automatic recording -> Host can pause/stop the auto recording in the cloud, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.5 Cloud recording downloads

1.2.5.1 Ensure cloud recording downloads is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Allow anyone with a link to the cloud recording to download

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording downloads, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Cloud recording downloads, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.5.2 Ensure only the host can download cloud recordings is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable "Only the host can download cloud recordings" option to block others to download the cloud recordings.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Only the host can download cloud recordings, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Only the host can download cloud recordings, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.6 Set minimum passcode strength requirements

1.2.6.1 Ensure have a minimum passcode length is set to 8 characters or greater (Manual)

Profile Applicability:

- Level 1

Description:

Have a minimum passcode length of 8 characters or greater

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> set to 8 characters or greater, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> set to 8 characters or greater, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.6.2 Ensure passcode have at least 1 letter is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Have at least 1 letter (a, b, c...)

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Have at least 1 letter (a, b, c...), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Have at least 1 letter (a, b, c...), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.6.3 Ensure passcode have at least 1 number is set to enabled (Manual)

Profile Applicability:

- Level 1

Description:

Have at least 1 number (1, 2, 3...)

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Have at least 1 number (1, 2, 3...), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Have at least 1 number (1, 2, 3...), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.6.4 Ensure passcode have at least 1 special character is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Have at least 1 special character (!, @, #...)

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Have at least 1 special character (!, @, #...), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Have at least 1 special character (!, @, #...), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.6.5 Ensure allow numeric passcode is set to disabled (Manual)

Profile Applicability:

- Level 1
- Level 2

Description:

Disable "Only allow numeric passcode"

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Only allow numeric passcode, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Set minimum passcode strength requirements -> Only allow numeric passcode, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.7 Recording disclaimer

1.2.7.1 Ensure recording disclaimer is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Show a customizable disclaimer to participants before a recording starts. Useful to address privacy requirements that mandates disclaimer prior recording starts.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Recording disclaimer, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Recording disclaimer, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.7.2 Ensure ask participants for consent when a recording starts is set to enabled (Manual)

Profile Applicability:

- Level 2
- Level 1

Description:

Ask participants for consent when a recording starts. Further click on "Customize" to modify the consent.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Recording disclaimer -> Ask participants for consent when a recording starts, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Recording disclaimer -> Ask participants for consent when a recording starts, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.7.3 Ensure ask host to confirm before starting a recording is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Ask host to confirm before starting a recording. Further click on "Customize" to modify the consent.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Recording disclaimer -> Ask host to confirm before starting a recording, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Recording disclaimer -> Ask host to confirm before starting a recording, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.8 Ensure prevent hosts from accessing their cloud recordings is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

By turning on this setting, the hosts cannot view their meeting cloud recordings. Only the admins who have recording management privilege can access them.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Prevent hosts from accessing their cloud recordings, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Prevent hosts from accessing their cloud recordings, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.9 Ensure IP address access control is set to organization approved ranges (Manual)

Profile Applicability:

- Level 2

Description:

Allow cloud recording access only from specific IP address ranges. This option can enable certain IP address range within the organization, to allow download of recording. Once enabled, provide the IP ranges.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> IP Address Access Control, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> IP Address Access Control, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.10 Ensure require passcode to access shared cloud recordings is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Passcode protection will be enforced for shared cloud recordings. A random passcode will be generated which can be modified by the users. This setting is applicable for newly generated recordings only.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Require passcode to access shared cloud recordings, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Require passcode to access shared cloud recordings, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.11 Ensure the host can delete cloud recordings is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow the host to delete the recordings. If this option is disabled, the recordings cannot be deleted by the host and only admin can delete them.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> The host can delete cloud recordings, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> The host can delete cloud recordings, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.12 Ensure allow recovery of deleted cloud recordings from trash is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Deleted cloud recordings will be kept in trash for 30 days. These files will not count as part of the total storage allowance. Useful when downloaded recordings are accidentally deleted.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Allow recovery of deleted cloud recordings from Trash, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Allow recovery of deleted cloud recordings from Trash, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.2.13 Ensure multiple audio notifications of recorded meeting is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Play notification messages to participants who join the meeting audio. These messages play each time the recording starts or restarts, informing participants that the meeting is being recorded. If participants join the audio from telephone, even if this option is disabled, users will hear one notification message per meeting. Useful to address privacy requirements that require recording disclaimer.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Multiple audio notifications of recorded meeting, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Recording -> Multiple audio notifications of recorded meeting, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.3 Telephone

1.3.1 Ensure toll call is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Include the selected numbers in the Zoom client and the email invitation via the international numbers link. Participants can dial into meeting with the numbers. Further add/modify/remove the toll numbers as per organization requirements.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Telephone -> Toll Call, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Telephone -> Toll Call, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.3.2 Ensure mask phone number in the participant list is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Phone numbers of users dialing into a meeting will be masked in the participant list. For example: 888****666

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Telephone -> Mask phone number in the participant list, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Telephone -> Mask phone number in the participant list, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

1.3.3 Ensure global dial-in countries/regions is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Click the Edit icon to choose countries/regions that frequently have participants who need to dial into meetings. The dial-in phone numbers of these locations appear in the email invitation, and can be used by participants dialing in from those locations. Further select Dial-in number(s) that are as per your local country or region laws, if any.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Telephone -> Global Dial-in Countries/Regions, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Account Settings -> Telephone -> Global Dial-in Countries/Regions, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2 IM Management

2.1 IM Settings

2.1.1 Sharing

2.1.1.1 Ensure screen capture is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to take and send screenshots in direct messages or group conversations. Reduces likelihood of data leakage through zoom screenshot sharing.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> Screen capture, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> Screen capture, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.1.2 Ensure code snippet is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to send bits of code, configuration files, or log files in direct messages or group conversations. Reduces likelihood of data leakage through zoom screenshot sharing.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> Code Snippet, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> Code Snippet, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.1.3 Ensure animated GIF images is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to search GIF images from Giphy. Reduces likelihood of data leakage through zoom screenshot sharing.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> Animated GIF images, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> Animated GIF images, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.1.4 Ensure file transfer is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to send and receive files in direct messages or group conversations. Reduces likelihood of data leakage through zoom screenshot sharing.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> File transfer, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Sharing -> File transfer, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.2 Visibility

2.1.2.1 Ensure set chat as a default tab for first-time users is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

By enabling this option, the default tab for first-time users will be switched from Home to Chat.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Set Chat as a default tab for first-time users, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Set Chat as a default tab for first-time users, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.2.2 Ensure show H.323 contacts is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

By enabling this option, the user's H.323 contacts will be displayed in the contact's list.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Show H.323 contacts, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Show H.323 contacts, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.2.3 Ensure company contacts is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

In your Zoom applications, the Contacts list will display all members of your account.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Company Contacts, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Company Contacts, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.2.4 Ensure IM groups is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

In your Zoom applications, the Contacts list will display all members of your account. For "Account Management -> IM Management -> IM Groups" option to work, this option need to be enabled.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Company Contacts, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> IM Groups, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.2.5 Ensure announcements is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow specified users to send one-way announcements to everyone in the same account.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Announcements, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Visibility -> Announcements, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.3 Security

2.1.3.1 Ensure enable advanced chat encryption is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Add an additional layer of encryption. Note that some features such as chat archives will be unavailable if this feature is enabled.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Enable advanced chat encryption, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Enable advanced chat encryption, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.3.2 Ensure enable personal channel in chat window is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

A personal channel allows users to save their private notes, action items, links, and files.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Enable Personal channel in Chat window, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Enable Personal channel in Chat window, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.3.3 Ensure allow users to add contacts is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

By disabling this setting, users will not be able to add contacts. If this option is required to be enabled, then choose "Only in the same organization and specified domains" and specify the domains for better security.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Allow users to add contacts, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Allow users to add contacts, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.3.4 Ensure allow users to chat with others is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

If you select 'Only in the same organization', users may still be able to chat with external users if they are added to channels or group chats with external users. If this option is required to be enabled, then choose "Only in the same organization and specified domains" and specify the domains for better security.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Allow users to chat with others, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Allow users to chat with others, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.3.5 Ensure show status to external contacts is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Status indicates the current availability (Available, Away, Do Not Disturb, In a Zoom meeting, Presenting) of users to their contacts. Choose whether or not external contacts can see your users' statuses.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Show status to external contacts, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Security -> Show status to external contacts, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.4 Storage

2.1.4.1 Ensure cloud storage is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Save messages and files on the cloud for the specified period of time. Select the number of years to store the data as per local laws.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Cloud storage, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Cloud storage, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.4.2 Ensure delete local data is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Specify how long your messages and files are saved on the local device.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Delete local data, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Delete local data, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.4.3 Ensure store edited and deleted message revisions is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Keep the original versions of edited and deleted messages on the Chat History tab.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Store edited and deleted message revisions, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Store edited and deleted message revisions, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.1.4.4 Ensure third party archiving is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Archive messages and files with a third party archiving service. Set up your account to send data to your archiving provider here.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Third party archiving, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Settings -> Storage -> Third party archiving, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

2.2 Enable IM groups is set to the organization's needs (Manual)

Profile Applicability:

- Level 2

Description:

IM Groups will be displayed in the Contacts section of your Zoom client. Creates groups as required.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Groups -> Add/Modify/Remove groups as per the organizations requirements.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> IM Management -> IM Groups -> Add/Modify/Remove groups as per the organizations requirements.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3 Advanced

3.1 Security

Go into the Zoom Admin Dashboard on the zoom website -> Advanced.

3.1.1 Authentication

3.1.1.1 Enhanced Password Requirement

3.1.1.1.1 Ensure minimum password length is set to 9 characters or greater (Manual)

Profile Applicability:

- Level 2

Description:

Have a minimum password length of 9 characters or greater

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> 9 characters or greater, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> 9 characters or greater, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.1.2 Ensure password have at least 1 special character is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Have at least 1 special character (!, @, #...)

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> Have at least 1 special character (!, @, #...), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> Have at least 1 special character (!, @, #...), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.1.3 Ensure password cannot contain consecutive characters is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Cannot contain consecutive characters (e.g. "11111", "12345", "abcde", or "qwert") and specify the length of consecutive characters to 4 or above.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> Cannot contain consecutive characters (e.g. "11111", "12345", "abcde", or "qwert"), and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> Cannot contain consecutive characters (e.g. "11111", "12345", "abcde", or "qwert"), and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.1.4 Ensure use enhanced weak password detection is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Use enhanced weak password detection.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> Use enhanced weak password detection, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Enhanced Password Requirement -> Use enhanced weak password detection, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.2 Password Policy

3.1.1.2.1 Ensure new users need to change their passwords upon first sign-in is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

New users need to change their passwords upon first sign-in.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> New users need to change their passwords upon first sign-in, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> New users need to change their passwords upon first sign-in, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.2.2 Ensure password expires automatically and needs to be changed after 365 days (Manual)

Profile Applicability:

- Level 2

Description:

Password expires automatically and needs to be changed after the specified number of days.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> Password expires automatically and needs to be changed after 365 days, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> Password expires automatically and needs to be changed after 365 days, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.2.3 Ensure users cannot reuse any password used in the last 5 times or more (Manual)

Profile Applicability:

- Level 2

Description:

Users cannot reuse any password used in the previous number of times.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> Users cannot reuse any password used in the last 5 times or more, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> Users cannot reuse any password used in the last 5 times or more, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.2.4 Enable users can change their password 1 time every 24 hours (Manual)

Profile Applicability:

- Level 2

Description:

Users can change their password 1 time every 24 hours.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> Users can change their password 1 time every 24 hours, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Password Policy -> Users can change their password 1 time every every 24 hours, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.3 Security

3.1.1.3.1 Ensure only account admin can change licensed users' personal meeting ID and personal link name (Manual)

Profile Applicability:

- Level 2

Description:

Only account admin can change licensed users' Personal Meeting ID and Personal Link Name. After enabling this option, further enable "Personal Meeting ID" and "Personal Link Name" and click save.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Security -> Only account admin can change licensed users' Personal Meeting ID and Personal Link Name, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Security -> Only account admin can change licensed users' Personal Meeting ID and Personal Link Name, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations
Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.3.2 Ensure allow importing of photos from the photo library on the user's device is set to disabled (Manual)

Profile Applicability:

- Level 2

Description:

Allow importing of photos from the photo library on the user's device.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Security -> Allow importing of photos from the photo library on the user's device, and check if it is disabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Security -> Allow importing of photos from the photo library on the user's device, and ensure it is disabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.1.1.3.3 Ensure hide billing information from administrators is set to enabled (Manual)

Profile Applicability:

- Level 2

Description:

Hide billing information from administrators.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Security -> Hide billing information from administrators, and check if it is enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Security -> Authentication -> Security -> Hide billing information from administrators, and ensure it is enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

3.2 Ensure integration is set to appropriate organizational needs (Manual)

Profile Applicability:

- Level 2

Description:

Integration, this page has option to enable/disable to various applications that can be integrated with zoom.

Rationale:

Audit:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Integration, and check if only necessary options are enabled.

Remediation:

Go into the Zoom Admin Dashboard on the zoom website. Account Management -> Advanced -> Integration, and ensure only necessary options are enabled.

CIS Controls:

Version 7

5.1 Establish Secure Configurations

Maintain documented, standard security configuration standards for all authorized operating systems and software.

Appendix: Summary Table

Control		Set Correctly	
		Yes	No
1	**Account Settings**		
1.1	**Meeting**		
1.1.1	**Security**		
1.1.1.1	**Passcode Requirement**		
1.1.1.1.1	Ensure minimum passcode length is set to at least 6 characters (Manual)	☐	☐
1.1.1.1.2	Ensure passcode is set to have at least 1 letter (Manual)	☐	☐
1.1.1.1.3	Ensure passcode is set to have at least 1 number (Manual)	☐	☐
1.1.1.1.4	Ensure passcode is set to have at least 1 special character (Manual)	☐	☐
1.1.1.1.5	Ensure passcode include both uppercase and lowercase characters is set to enabled (Manual)	☐	☐
1.1.1.1.6	Ensure passcode cannot contain consecutive characters is set to enabled (Manual)	☐	☐
1.1.1.1.7	Ensure enhanced weak passcode detection is set to enabled (Manual)	☐	☐
1.1.1.1.8	Ensure only allow numeric passcode is set to disabled (Manual)	☐	☐
1.1.1.2	Ensure waiting room is set to enabled (Manual)	☐	☐
1.1.1.3	Ensure waiting room options is set to everyone (Manual)	☐	☐
1.1.1.4	Ensure require a passcode when scheduling new meetings is set to enabled (Manual)	☐	☐
1.1.1.5	Ensure room meeting ID passcode is set to enabled (Manual)	☐	☐
1.1.1.6	Ensure require a password for instant meetings is set to enabled (Manual)	☐	☐
1.1.1.7	Ensure require a password for Personal Meeting ID (PMI) is set to enabled (Manual)	☐	☐
1.1.1.8	Ensure embed password in meeting link for one-click join is set to enabled (Manual)	☐	☐
1.1.1.9	Ensure only authenticated users can join meetings is set to enabled (Manual)	☐	☐
1.1.1.10	Ensure require password for participants joining by phone is set to enabled (Manual)	☐	☐
1.1.1.11	Ensure only authenticated users can join meetings from Web client is set to enabled (Manual)	☐	☐
1.1.2	**Schedule Meeting**		

1.1.2.1	**Meeting password requirement**		
1.1.2.1.1	Have a minimum password length (Automated)	☐	☐
1.1.2.1.2	Specify a password length: (Automated)	☐	☐
1.1.2.1.3	Have at least 1 letter (a, b, c...) (Automated)	☐	☐
1.1.2.1.4	Have at least 1 number (1, 2, 3...) (Automated)	☐	☐
1.1.2.1.5	Have at least 1 special character (!, @, #...) (Manual)	☐	☐
1.1.2.1.6	Include both uppercase and lower case letters (Automated)	☐	☐
1.1.2.2	Ensure host video is set to disabled (Manual)	☐	☐
1.1.2.3	Ensure participants video is set to disabled (Manual)	☐	☐
1.1.2.4	Ensure join before host is set to disabled (Automated)	☐	☐
1.1.2.5	Ensure enable personal meeting ID is set to enabled (Manual)	☐	☐
1.1.2.6	Ensure use personal meeting ID (PMI) when scheduling a meeting is set to disabled (Manual)	☐	☐
1.1.2.7	Ensure use personal meeting ID (PMI) when starting an instant meeting is set to disabled (Manual)	☐	☐
1.1.2.8	Ensure add watermark is set to enabled (Manual)	☐	☐
1.1.2.9	Ensure add audio watermark is set to enabled (Manual)	☐	☐
1.1.2.10	Ensure always display "Zoom Meeting" as the meeting topic is set to enabled (Manual)	☐	☐
1.1.2.11	Ensure bypass the password when joining meetings from meeting list is set to enabled (Manual)	☐	☐
1.1.2.12	Ensure mute participants upon entry is set to enabled (Manual)	☐	☐
1.1.2.13	Ensure upcoming meeting reminder is set to enabled (Manual)	☐	☐
1.1.3	**In Meeting (Basic)**		
1.1.3.1	**Chat**		
1.1.3.1.1	Ensure allow meeting participants to send a message visible to all participants is set to disabled (Manual)	☐	☐
1.1.3.1.2	Ensure prevent participants from saving chat is set to enabled (Manual)	☐	☐
1.1.3.2	**Sound notification when someone joins or leaves**		
1.1.3.2.1	Ensure sound notification when someone joins or leaves is set to enabled (Manual)	☐	☐
1.1.3.2.2	Ensure play sound for "Host and co-host only" is set to enabled (Manual)	☐	☐
1.1.3.2.3	Ensure when someone joins by phone, ask to record their voice to use as the notification is set to enabled (Manual)	☐	☐
1.1.3.3	**File transfer**		
1.1.3.3.1	Ensure hosts and participants can send files through the in-meeting chat is set to disabled (Manual)	☐	☐

1.1.3.3.2	Ensure only allow specified file types is set to enabled (Manual)	☐	☐
1.1.3.4	**Screen sharing**		
1.1.3.4.1	Ensure screen sharing is set to enabled (Manual)	☐	☐
1.1.3.4.2	Ensure "who can share?" is set to "Host Only" (Manual)	☐	☐
1.1.3.4.3	Ensure "Who can start sharing when someone else is sharing?" is set to "Host Only" (Manual)	☐	☐
1.1.3.5	**Annotation**		
1.1.3.5.1	Ensure annotation is set to disabled (Manual)	☐	☐
1.1.3.5.2	Ensure allow saving of shared screens with annotations is set to disabled (Manual)	☐	☐
1.1.3.5.3	Ensure only the user who is sharing can annotate is set to enabled (Manual)	☐	☐
1.1.3.6	**Whiteboard**		
1.1.3.6.1	Ensure whiteboard is set to disabled (Manual)	☐	☐
1.1.3.6.2	Ensure allow saving of whiteboard content is set to disabled (Manual)	☐	☐
1.1.3.6.3	Ensure auto save whiteboard content when sharing is stopped is set to disabled (Manual)	☐	☐
1.1.3.7	Ensure require encryption for 3rd party endpoints (SIP/H.323) is set to enabled (Manual)	☐	☐
1.1.3.8	Ensure allow meeting participants to send a private 1:1 message to another participant is set to disabled (Manual)	☐	☐
1.1.3.9	Ensure auto saving chats is set to enabled (Manual)	☐	☐
1.1.3.10	Ensure feedback to Zoom is set to enabled (Manual)	☐	☐
1.1.3.11	Ensure co-host is set to enabled (Manual)	☐	☐
1.1.3.12	Ensure polling is set to enabled (Manual)	☐	☐
1.1.3.13	Ensure always show meeting control toolbar is set to enabled (Manual)	☐	☐
1.1.3.14	Ensure show Zoom windows during screen share is set to enabled (Manual)	☐	☐
1.1.3.15	Ensure disable desktop/screen share for users is set to enabled (Manual)	☐	☐
1.1.3.16	Ensure remote control is set to disabled (Manual)	☐	☐
1.1.3.17	Ensure nonverbal feedback is set to disabled (Manual)	☐	☐
1.1.3.18	Ensure meeting reactions is set to disabled (Manual)	☐	☐
1.1.3.19	Ensure allow removed participants to rejoin is set to disabled (Manual)	☐	☐
1.1.3.20	Ensure allow participants to rename themselves is set to enabled (Manual)	☐	☐
1.1.3.21	Ensure hide participant profile pictures in a meeting is set to disabled (Manual)	☐	☐
1.1.4	**In Meeting (Advanced)**		

1.1.4.1	**Select data center regions for meetings/webinars hosted by your account**		
1.1.4.1.1	Ensure select data center regions for meetings/webinars hosted by your account is set to enabled (Manual)	☐	☐
1.1.4.1.2	Ensure data center regions is set to local countries (Manual)	☐	☐
1.1.4.2	**Breakout room**		
1.1.4.2.1	Ensure breakout room is set to enabled (Manual)	☐	☐
1.1.4.2.2	Ensure allow host to assign participants to breakout rooms when scheduling is set to enabled (Manual)	☐	☐
1.1.4.3	**Virtual background**		
1.1.4.3.1	Ensure virtual background is set to enabled (Manual)	☐	☐
1.1.4.3.2	Ensure allow use of videos for virtual backgrounds is set to disabled (Manual)	☐	☐
1.1.4.3.3	Ensure allow users to upload custom backgrounds is set to disabled (Manual)	☐	☐
1.1.4.4	**Peer to Peer connection while only 2 people in a meeting**		
1.1.4.4.1	Ensure peer to peer connection while only 2 people in a meeting is set to disabled (Manual)	☐	☐
1.1.4.4.2	Enable listening ports range is set as appropriate for organization (Manual)	☐	☐
1.1.4.5	Ensure report participants to Zoom is set to enabled (Manual)	☐	☐
1.1.4.6	Ensure remote support is set to disabled (Manual)	☐	☐
1.1.4.7	Ensure closed captioning is set to disabled (Manual)	☐	☐
1.1.4.8	Ensure save captions is set to disabled (Manual)	☐	☐
1.1.4.9	Ensure far end camera control is set to disabled (Manual)	☐	☐
1.1.4.10	Ensure identify guest participants in the meeting/webinar is set to enabled (Manual)	☐	☐
1.1.4.11	Ensure auto-answer group in chat is set to disabled (Manual)	☐	☐
1.1.4.12	Ensure only show default email when sending email invites is set to enabled (Manual)	☐	☐
1.1.4.13	Ensure use HTML format email for Outlook plugin is set to enabled (Manual)	☐	☐
1.1.4.14	Ensure show a "Join from your browser" link is set to enabled (Manual)	☐	☐
1.1.4.15	Ensure allow live streaming meetings is set to disabled (Manual)	☐	☐
1.1.4.16	Ensure allow Skype for Business (Lync) client to join a Zoom meeting is set to disabled (Manual)	☐	☐
1.1.4.17	Ensure request permission to unmute is set to enabled (Manual)	☐	☐
1.1.5	**Calendar and Contacts**		

1.1.5.1	Ensure calendar and contacts integration is set to disabled (Manual)	☐	☐
1.1.5.2	Ensure ask users to integrate Office 365 calendar when they sign in is set to disabled (Manual)	☐	☐
1.1.5.3	Ensure consent to Office 365 calendar integration permissions on behalf of entire account is set to disabled (Manual)	☐	☐
1.1.5.4	Ensure enforce OAuth 2.0 for Office 365 calendar integration is set to enabled (Manual)	☐	☐
1.1.6	**Email Notification**		
1.1.6.1	**When a cloud recording is available**		
1.1.6.1.1	Ensure when a cloud recording is available is set to enabled (Manual)	☐	☐
1.1.6.1.2	Ensure Send a copy to the person who scheduled the meeting/webinar for the host is set to enabled (Manual)	☐	☐
1.1.6.1.3	Ensure send a copy to the Alternative Hosts is set to enabled (Manual)	☐	☐
1.1.6.2	Ensure when attendees join meeting before host is set to enabled (Manual)	☐	☐
1.1.6.3	Ensure when a meeting is cancelled is set to enabled (Manual)	☐	☐
1.1.6.4	Ensure when an alternative host is set or removed from a meeting is set to enabled (Manual)	☐	☐
1.1.6.5	Enable when someone scheduled a meeting for a host is set to enabled (Manual)	☐	☐
1.1.6.6	Ensure when the cloud recording is going to be permanently deleted from trash is set to enabled (Manual)	☐	☐
1.1.7	**Admin Options**		
1.1.7.1	Ensure blur snapshot on iOS task switcher is set to enabled (Manual)	☐	☐
1.1.7.2	Ensure display meetings scheduled for others is set to enabled (Manual)	☐	☐
1.1.7.3	Ensure use content delivery network (CDN) is set to "Default" (Manual)	☐	☐
1.1.7.4	Ensure allow users to contact Zoom's support via chat is set to enabled (Manual)	☐	☐
1.2	**Recording**		
1.2.1	**Local recording**		
1.2.1.1	Ensure local recording is set to enabled (Manual)	☐	☐
1.2.1.2	Ensure hosts can give participants the permission to record locally is set to enabled (Manual)	☐	☐
1.2.2	**Cloud recording**		
1.2.2.1	Ensure cloud recording is set to enabled (Manual)	☐	☐

1.2.2.2	Ensure record active speaker with shared screen is set to enabled (Manual)	☐	☐
1.2.2.3	Ensure record gallery view with shared screen is set to enabled (Manual)	☐	☐
1.2.2.4	Ensure record active speaker, gallery view and shared screen separately is set to enabled (Manual)	☐	☐
1.2.2.5	Ensure record an audio only file is set to enabled (Manual)	☐	☐
1.2.2.6	Ensure save chat messages from the meeting / webinar is set to enabled (Manual)	☐	☐
1.2.3	**Advanced cloud recording settings**		
1.2.3.1	Ensure add a timestamp to the recording is set to enabled (Manual)	☐	☐
1.2.3.2	Ensure display participants' names in the recording is set to enabled (Manual)	☐	☐
1.2.3.3	Ensure record thumbnails when sharing is set to enabled (Manual)	☐	☐
1.2.3.4	Ensure optimize the recording for 3rd party video editor is set to enabled (Manual)	☐	☐
1.2.3.5	Ensure save panelist chat to the recording is set to enabled (Manual)	☐	☐
1.2.4	**Automatic recording**		
1.2.4.1	Ensure automatic recording is set to enabled (Manual)	☐	☐
1.2.4.2	Ensure automatic recording is set to "Record in the Cloud" (Manual)	☐	☐
1.2.4.3	Ensure host can pause/stop the auto recording in the cloud is set to enabled (Manual)	☐	☐
1.2.5	**Cloud recording downloads**		
1.2.5.1	Ensure cloud recording downloads is set to enabled (Manual)	☐	☐
1.2.5.2	Ensure only the host can download cloud recordings is set to enabled (Manual)	☐	☐
1.2.6	**Set minimum passcode strength requirements**		
1.2.6.1	Ensure have a minimum passcode length is set to 8 characters or greater (Manual)	☐	☐
1.2.6.2	Ensure passcode have at least 1 letter is set to enabled (Manual)	☐	☐
1.2.6.3	Ensure passcode have at least 1 number is set to enabled (Manual)	☐	☐
1.2.6.4	Ensure passcode have at least 1 special character is set to enabled (Manual)	☐	☐
1.2.6.5	Ensure allow numeric passcode is set to disabled (Manual)	☐	☐
1.2.7	**Recording disclaimer**		
1.2.7.1	Ensure recording disclaimer is set to enabled (Manual)	☐	☐

1.2.7.2	Ensure ask participants for consent when a recording starts is set to enabled (Manual)	☐	☐
1.2.7.3	Ensure ask host to confirm before starting a recording is set to enabled (Manual)	☐	☐
1.2.8	Ensure prevent hosts from accessing their cloud recordings is set to enabled (Manual)	☐	☐
1.2.9	Ensure IP address access control is set to organization approved ranges (Manual)	☐	☐
1.2.10	Ensure require passcode to access shared cloud recordings is set to enabled (Manual)	☐	☐
1.2.11	Ensure the host can delete cloud recordings is set to disabled (Manual)	☐	☐
1.2.12	Ensure allow recovery of deleted cloud recordings from trash is set to enabled (Manual)	☐	☐
1.2.13	Ensure multiple audio notifications of recorded meeting is set to enabled (Manual)	☐	☐
1.3	**Telephone**		
1.3.1	Ensure toll call is set to enabled (Manual)	☐	☐
1.3.2	Ensure mask phone number in the participant list is set to enabled (Manual)	☐	☐
1.3.3	Ensure global dial-in countries/regions is set to enabled (Manual)	☐	☐
2	**IM Management**		
2.1	**IM Settings**		
2.1.1	**Sharing**		
2.1.1.1	Ensure screen capture is set to disabled (Manual)	☐	☐
2.1.1.2	Ensure code snippet is set to disabled (Manual)	☐	☐
2.1.1.3	Ensure animated GIF images is set to disabled (Manual)	☐	☐
2.1.1.4	Ensure file transfer is set to disabled (Manual)	☐	☐
2.1.2	**Visibility**		
2.1.2.1	Ensure set chat as a default tab for first-time users is set to disabled (Manual)	☐	☐
2.1.2.2	Ensure show H.323 contacts is set to disabled (Manual)	☐	☐
2.1.2.3	Ensure company contacts is set to disabled (Manual)	☐	☐
2.1.2.4	Ensure IM groups is set to enabled (Manual)	☐	☐
2.1.2.5	Ensure announcements is set to disabled (Manual)	☐	☐
2.1.3	**Security**		
2.1.3.1	Ensure enable advanced chat encryption is set to enabled (Manual)	☐	☐
2.1.3.2	Ensure enable personal channel in chat window is set to disabled (Manual)	☐	☐
2.1.3.3	Ensure allow users to add contacts is set to disabled (Manual)	☐	☐

2.1.3.4	Ensure allow users to chat with others is set to disabled (Manual)	☐	☐
2.1.3.5	Ensure show status to external contacts is set to disabled (Manual)	☐	☐
2.1.4	**Storage**		
2.1.4.1	Ensure cloud storage is set to enabled (Manual)	☐	☐
2.1.4.2	Ensure delete local data is set to disabled (Manual)	☐	☐
2.1.4.3	Ensure store edited and deleted message revisions is set to disabled (Manual)	☐	☐
2.1.4.4	Ensure third party archiving is set to disabled (Manual)	☐	☐
2.2	Enable IM groups is set to the organization's needs (Manual)	☐	☐
3	**Advanced**		
3.1	**Security**		
3.1.1	**Authentication**		
3.1.1.1	**Enhanced Password Requirement**		
3.1.1.1.1	Ensure minimum password length is set to 9 characters or greater (Manual)	☐	☐
3.1.1.1.2	Ensure password have at least 1 special character is set to enabled (Manual)	☐	☐
3.1.1.1.3	Ensure password cannot contain consecutive characters is set to enabled (Manual)	☐	☐
3.1.1.1.4	Ensure use enhanced weak password detection is set to enabled (Manual)	☐	☐
3.1.1.2	**Password Policy**		
3.1.1.2.1	Ensure new users need to change their passwords upon first sign-in is set to enabled (Manual)	☐	☐
3.1.1.2.2	Ensure password expires automatically and needs to be changed after 365 days (Manual)	☐	☐
3.1.1.2.3	Ensure users cannot reuse any password used in the last 5 times or more (Manual)	☐	☐
3.1.1.2.4	Enable users can change their password 1 time every 24 hours (Manual)	☐	☐
3.1.1.3	**Security**		
3.1.1.3.1	Ensure only account admin can change licensed users' personal meeting ID and personal link name (Manual)	☐	☐
3.1.1.3.2	Ensure allow importing of photos from the photo library on the user's device is set to disabled (Manual)	☐	☐
3.1.1.3.3	Ensure hide billing information from administrators is set to enabled (Manual)	☐	☐
3.2	Ensure integration is set to appropriate organizational needs (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version