GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Updated Zoom Security Guidance

Securing Zoom for Government Use

Purpose

1. This paper sets out the Government Chief Information Security Officer's (GCISO) guidance on important security considerations when using Zoom remote conferencing services for official New Zealand Government business, either within a public sector agency, or when collaborating with partner organisations.

2. This paper follows on from our previous 'End User Guidance' loaded to the NCSC website on April 1 2020, and the more detailed 'Agencies' Technical Guidance' distributed directly to CISOs on 27 March 2020.

3. This paper provides new guidance to the public sector, which is based on further research and security analysis undertaken in the intervening period. It reflects the most recent product updates within Zoom itself, and provides further technical recommendations for securing Zoom for New Zealand Government business. This guidance should be read in conjunction with our advice on working from home, and in particular our principles for secure video, voice, and messaging communications. The intention of this guidance, along with our more detailed analysis of Zoom, is to assist agencies in returning to normal business practices and processes at COVID-19 alert level 2

4. As per our previous guidance released on Zoom, under no circumstances should Zoom be used when dealing with information classified above RESTRICTED.

Why the need for this updated guidance?

5. This updated guidance provides information on how agencies should progress their security-related work associated with Zoom at the onset of COVID-19 alert level 2 on 14 May.

6. Our previous guidance was provided largely for those agencies who had been unable to undertake certification and accreditation before using Zoom, and was applicable during COVID-19 alert levels 3 and 4 for the period 23 March to 13 May 2020. From 14 May, our previous guidance will not apply.

7. This means that agencies will not be able to rely on our previous guidance as the basis for using Zoom when the country moves out of the COVID-19 alert level 3 lockdown on 14 May.

8. This new guidance outlines what agencies need to consider if they intend to continue to use Zoom as New Zealand moves out of COVID-19 lockdown. Zoom should be used in accordance with agencies' normal business practices, policies and standards for video conferencing tools. At a practical level, we are conscious that agencies are all positioned differently in terms of how to use Zoom in their respective operating environments and business contexts. This guidance is intended to assist agencies in making their respective shifts to COVID-19 alert level 2 and subsequent alert levels, now that they are better disposed to consider and assess the risks posed by using Zoom

9. This guidance also provides a greater degree of analysis around security settings and documentation, which is intended to assist agencies in making decisions and implementing standards for the use of Zoom in the future.

10. Due to the constant security changes within the Zoom platform, our previous guidance will not come back into effect should the country enter levels 3 or 4 in the future. Also, due to the range and pace of these security changes, our guidance no longer contains detailed information on specific user settings, as these are prone to frequent changes and updates.

Can I continue to use Zoom?

11. The decision to continue to use Zoom will ultimately be made at an agency level, based on the agency's context and the intended use of the Zoom platform.

12. Public sector agencies have largely been working remotely for a number of weeks in March and April. COVID-19 alert levels 3 and 4 have required different ways of working for many agencies, including a significant increase in the use of video conferencing software such as Zoom. This is unlikely to change substantially as New Zealand moves to COVID-19 level 2. However, the ways in which agencies use video conferencing software will be different depending on each agency's context.

13. The NZISM sets out that agencies must conduct a certification and accreditation (C&A) process when deploying new systems and software. This is a time-intensive process that agencies may not have been able to undertake in order to deploy Zoom to staff and stakeholders in the timeframes available at the outset of the alert level 4 lockdown in March.

14. If your agency has not been able to undertake certification and accreditation before using Zoom, you should now take the opportunity as New Zealand moves to COVID-19 alert level 2 to implement appropriate controls to mitigate the risks posed by the use of Zoom. You should also put a plan in place for how you will scale up security activities to mitigate risks, and to ensure that you are now working towards completing C&A for any newly introduced teleconferencing platforms.

    If your agency intends to continue using Zoom, you should:

    - assess whether your context and requirement for Zoom use is still fit for purpose;
    - carry out a risk assessment if you elect to continue using Zoom for future business purposes (the following sections in this guidance outline some common risks to assist in this assessment);
    - make an in-principle decision if you are going to use Zoom (or not);
    - continue to maintain the good security practices set out in this guidance;

- implement appropriate controls to mitigate the risks of continued Zoom use, if you have not already been able to do so;
- commence certification and accreditation processes as required by the NZISM, as soon as practicable;
- ask for help if you need it (there are a number of agencies that have full risk assessment and certification documentation you can seek help from);
- ensure that your system administrators stay up-to-date with Zoom's continued improvement of its privacy, security and safety features and user settings, and ensure that your system administrators are aware of future updates and patches and take steps to readily implement these;
- conduct checks to see that Zoom has moved to AES 256 on 30 May;
- continue to prioritise the use of video conferencing tools that have already been subjected to a security risk assessment and C&A process, in line with your organisation's policies and standards.

Security risks associated with Zoom for agencies' consideration

15. As with any other software, there is a suite of security risks associated with using video conferencing tools. The NZISM sets out relevant controls and expectations for video conferencing tools like Zoom in the following chapters:
    a. Chapter 18.3: Video & Telephony Conferencing and Internet Protocol Telephony
    b. Chapter 12: Product Security
    c. Chapter 11: Communications Systems and Devices
    d. Chapter 19: Gateways Security
16. Below is a list of commonly identified risks associated with Zoom. These should be considered and assessed against your agency's specific risk framework when conducting the C&A required for Zoom use in your agency. Please note: this is not a full or comprehensive list.

Risks to consider when using Zoom
Device compromise A Zoom-enabled device is compromised and remotely controlled. Video camera or microphones used to record meetings or surrounding environment, leading to security breach, data loss, and reputational damage.
Zoom device is used to attack other internal systems A compromised Zoom-enabled device is used to attack internal systems, leading to further security breach, data loss, and reputational damage.
Interception of communication Zoom communications are intercepted and compromised (in real time) leading to security breach and reputational damage.

Stored video recordings are stolen Stored Zoom communications are accessed by unauthorised means, leading to potential security breach and reputational damage.
Unauthorised access to a Zoom meeting An unauthorised person may be able to obtain information about the video conference conversations due to a lack of identity access management. This may result in unauthorised access to personal information sent between the host and invitee of the video call.
Insider threat If a malicious Zoom administrator misuses their access rights, it may result in: • unauthorised access to data or systems; • data alteration; • data disclosure; • widespread loss of data or system access. Similar risks apply to accidental action from administrators and users.
Degradation of service or denial of service The service may become unreliable due to a failure by Zoom to manage and support the video conferencing solution. This may result in: • inappropriate access (including cross tenancy); • unwanted data disclosure; • loss of data integrity; • availability impacts.
Inappropriate sharing of classified information An official sends classified information to a recipient using the 'share document' feature within the Zoom application.

17. It should be noted that you need to complete a risk assessment for your use of the system within your own context. You may have identified risks not listed in the above table, and some risks may not apply to you. Below is our updated and recommend guidance on using Zoom. This guidance will assist you to begin securing Zoom for your agency's use. Please note: this is not an exhaustive list of controls. Our recent analysis

ZOOM 5.0 updates

18. Zoom is undergoing considerable and constant change to meet the demands of its rapidly growing customer base in recent months. We carried out further analysis on the most recent Zoom 5.0 updates, and this provided the basis for our updated recommendations for securing Zoom as agencies move out of COVID-19 level 3.

19. On 28 April 2020, Zoom released Zoom version 5.0 and began rolling out patch updates to all Zoom desktop and mobile applications. We have reviewed Zoom

version 5.0 to determine whether it addresses our concerns around encryption and server infrastructure.

20. Despite moving to AES 256 from 128-bit AES, Zoom still uses ECB mode. We note that Zoom intends on shifting to Galois/Counter Mode (GCM) on 30 May 2020.

21. Zoom now allows paying users to determine the network region(s) that their data is routed through. This is an improvement from previously allowing routing through any country, but falls short of applying to all users.

22. Zoom meeting IDs have been lengthened to mitigate against attackers targeting them, and meeting passwords are now mandatory. However, the default passwords themselves are weak (only 6 characters, or 36 bits of entropy). Administrators can apply stronger passwords, which we would recommend.

23. Other new features include:

    a. meeting admins/organisers control who can enter the meeting and can kick users out of the meeting;

    b. meeting admins/organisers are privy to all chat correspondence exchanged within the meeting, even if it is not intended for them.

Our recommendations for securing Zoom

Have a paid Zoom subscription for your agency?

24. Zoom has a number of settings and security improvements that are only available for paid subscribers. Your agency should have a paid subscription that is appropriate for your user base and needs.

Authentication

25. We recommend that you integrate Zoom with your agency's single sign-on (SSO) solution (e.g. Azure AD or Okta). Using your existing SSO solution will better enable you to manage MFA as well as user on-boarding and off-boarding, rather than relying solely on Zoom's internal MFA option.

26. If you do not have an SSO solution that can integrate with Zoom, you should provide the standard guidance to your users about setting long, strong and unique passwords for their Zoom accounts.

Update Zoom to the newest version as soon as possible

27. Updating to the latest version of software is common, well-understood security advice.

28. At the time of writing (April-May 2020), Zoom is undergoing a 90-day privacy and security uplift. For example, version 5 of Zoom (released 28 April) has incorporated a number of necessary security updates.

29. We recommend system administrators update to the most recent version of Zoom as soon as is practicable.

Apply operational security mitigations

30. As an administrator, you can configure Zoom to increase its security. You can set your password requirements (long and strong) and other security settings (such as requiring

MFA). Implement what you can to comply with NZISM standards as soon as possible and review the security panel routinely as changes will likely occur over time.

31. More information about the security settings can be found here: https://support.zoom.us/hc/en-us/articles/360034675592-Advanced-security-settings

Manage Zoom server locations

32. Paid subscribers of Zoom can now select which network regions their Zoom meetings use for hosting and key management.

33. We recommend you review these regions and de-select those regions which you are not comfortable with your meeting data being located in. Note that at the time of writing this advice, the closest Zoom network region to New Zealand is Australia.

Additional mitigations

34. We acknowledge the implementation of mitigations is dependent on your business context and needs, and it may not be practical to implement them all. You should try to implement the mitigations that are practical as soon as possible. The below list is presented in order of priority.

Device monitoring

35. We recommend you implement or broaden device monitoring and logging to aid you in security monitoring and incident response in the coming weeks and months.

36. As per our principles for implementing cloud technologies at pace, it is important that you log as much as you can, whether or not you have the capacity to monitor it when you turn on logging.

Device hardening

37. If possible, Zoom should be used on a work device. You may not be able to harden devices immediately without existing remote access due to social distancing and isolation restrictions.

For further information, please email info@ncsc.govt.nz