

## Tips om ZOOM Meetings te beveiligen

Door de explosie in zoomgebruik heeft ZOOM snel de toegankelijkheid van privacy- en beveiligingsfuncties aangepakt en alle beveiligingsopties in de werkbalk toegevoegd. Het is echter belangrijk om ervoor te zorgen dat de host/mediator deze veiligheidsopties goed gebruikt.

**Updates bijwerken:** Na een updatemelding van Zoom wordt deze meteen bijgewerkt zodat we verzekerd zijn van de allerlaatste veiligheidsupdate. Als de zoom-app niet is bijgewerkt, kunt u de nieuwste versie downloaden en opnieuw installeren.

**Beveiligingsopties in de werkbalk.** De host heeft een beveiligingspictogram onder in de werkbalk voor snelle toegang tot de essentiële beveiligingsmaatregelen tijdens vergaderingen.

**Vergrendel zoomvergaderingen:** Wanneer een host een Zoom Meeting vergrendelt die al is gestart, kunnen geen nieuwe deelnemers deelnemen, zelfs niet als ze de meeting-ID en het wachtwoord hebben (als u er een nodig heeft).

**Video uitschakelen:** De host kan iemands video uitschakelen.

**Wachtkamer:** Schakel 'Deelnemen vóór host' uit en schakel voor elke vergadering een 'Wachtkamer' in om de controle over de vergadering te behouden. De host geeft zelf akkoord om iemand vervolgens toe te laten tot de vergadering.

**Deelnemer in de wacht zetten:** De host kan een deelnemer in de wacht zetten en de video- en audioverbindingen wordt tijdelijk uitgeschakeld.

**Wachtwoord om deel te nemen aan de vergadering:** Maak afzonderlijke wachtwoorden om elke vergadering te beveiligen.

**Muten:** De host kan individuele deelnemers of allemaal tegelijk muten/unmuten. Ongewenst, storend of ongepast geluid van andere deelnemers kan de host blokkeren. U kunt "Mute Upon Entry" ook inschakelen in uw instellingen, wat een goede optie is voor grote vergaderingen.

**Deelnemers verwijderen:** In het deelnemersmenu kunt u met de muis over de naam van een deelnemer bewegen en er zullen verschillende opties verschijnen, waaronder "Verwijderen".

**Annotatie uitschakelen:** U kunt de annotatiefunctie uitschakelen in uw zoominstellingen om te voorkomen dat mensen over de schermen schrijven.

**Schakel bestandsoverdracht uit:** Met bestandsoverdracht tijdens vergaderingen kunnen mensen bestanden delen via de chat in vergadering. Schakel dit uit zodat geen gevoelige bestanden kunnen worden gedeeld.

**Schermdelen:** De host van de vergadering kan het delen van schermen voor deelnemers uitschakelen.

**Controle opname:** De mogelijkheid om op te nemen in de cloud of lokaal is iets dat een account owner kan bepalen. Als ze opnametoegang hebben, kan de host beslissen om een deelnemer of alle deelnemers in te schakelen / uit te schakelen.

**Privéchat uitschakelen:** Zoom heeft in-meeting chat voor iedereen óf deelnemers kunnen elkaar privé berichten sturen. Beperk het vermogen van deelnemers om met elkaar te chatten terwijl uw vergadering/evenement gaande is en beperk afleiding.

#### **Tot slot:**

- Deel de vergaderingslink, vergaderings-ID of foto's met de vergaderings-ID niet op openbare platforms (a la Boris Johnson).
- Schakel 'Sta verwijderde deelnemers toe om opnieuw deel te nemen' uit om ongewenste partijen buiten vergaderingen te houden
- Zodra iedereen in de vergadering is, vergrendelt de host vergadering om te voorkomen dat ongewenste partijen binnenkomen.