PANDUAN KEAMANAN PEMANFAATAN VIDEO CONFERENCE (*VC*): UPAYA MENCEGAH PENYUSUP DAN MELINDUNGI DATA PRIBADI

BELAJAR DARI KASUS *VC* WANTIKNAS TANGGAL 16 APRIL 2020

ASDEP TELEMATIKA DAN UTILITAS
MENKO PEREKONOMIAN

I. TATA CARA PENYELENGGARAAN *VC* DASAR (BSSN)

Panduan ini berisi tata cara penyelenggaraan pertemuan jarak jauh (telekonferensi) melalui *video conference* (*VC*) dengan tetap memperhatikan keamanan informasi, antara lain membahas: A. Penyiapan Sarana; B. Langkah-langkah Pengamanan; dan C. *Best Practice*. Bahan disarikan dari **Imbauan Keamanan Pemanfaatan Aplikasi *Video Conference*** oleh BSSN.

A.PENYIAPAN SARANA

1. Aplikasi *Video Conference (VC)*

a. Disarankan menggunakan aplikasi *VC* yang resmi/ berlangganan dan merupakan versi terbaru dan diunduh dari sumber resmi.
b. Untuk sektor publik disarankan *server* aplikasi berada pada organisasi pengguna dan dikelola secara mandiri (*on-premise*), atau jika belum demikian agar menggunakan aplikasi dengan pengelolaan *server* berada di dalam wilayah Indonesia terkecuali untuk sektor *private* (PP 71/ 2019).
c. Jika server aplikasi berada di dalam organisasi sebaiknya dikonfigurasi untuk jaringan local dan setiap partisipan yang ingin bergabung wajib memiliki akses VPN (*Virtual Private Network*).
d. Diusahakan menggunakan aplikasi yang memiliki fitur enkripsi, *end-to-end encryption*, *private chat, link communication,* atau sejenisnya dan dapat diaktifkan pada saat telekonferensi berlangsung.
e. Pilih aplikasi yang memiliki fitur pembatasan/ *waiting* pada saat seluruh partisipan telah bergabung di *VC,* untuk menghindari pengguna lain masuk tanpa ada konfirmasi terlebih dahulu.
f. Agar dipastikan *ID, PIN atau Password* selalu diperbarui dan diganti setiap pelaksanaan rapat.
g. Pastikan akun yg digunakan adalah akun resmi dinas/ akun milik pribadi.
h. Pastikan nama profil sesuai dengan yang disepakati sehingga mempermudah melakukan kontrol terhadap partisipan yang tergabung.
i. Pastikan aplikasi/ peserta *VC* mendapat/ meminta izin ketika mengaktifkan kamera atau mikrofon, dan pastikan tidak ada permintaan akses kamera atau mikrofon yang tersembunyi.

2. Perangkat dan Komunikasi

a. **Sisi *Host***:
   1) Gunakan kata kunci yang kuat (min 8 karakter kombinasi huruf besar kecil dan karakter khusus) untuk *password VC.*
   2) ID/ *Username* dan *password* rapat didistribusikan secara aman kepada partisipan undangan dengan melakukan *invite* lewat email/ media yang terpercaya, tidak secara publik (min 20 menit sebelum rapat dimulai).
   3) Jika ada, aktifkan (*enable*) fitur ‘pembatasan’ (*waiting room*) pada saat seluruh partisipan telah bergabung di *VC*, untuk menghindari pengguna

lain masuk tanpa ada konfirmasi terlebih dahulu.

4) Pastikan ID rapat dan *password* selalu diperbarui dan diganti setiap pelaksanaan rapat.
5) Pastikan perangkat yang digunakan sudah terpasang antivirus dan *firewall* yang diperbaharui secara berkala.
6) Lakukan monitoring dan verifikasi terhadap setiap partisipan yang telah dan akan bergabung pada *VC*.
7) Selalu evaluasi keamanan yang telah dilakukan demi mendapatkan hasil rapat bersama yang aman dan nyaman bagi semua.

b. **Sisi *Client/ Participant:***

1) Selalu gunakan Perangkat (*device)* milik pribadi tidak publik/ umum.
2) Sebelum rapat selalu siap (*standby*) membuka email/ media lain terpercaya untuk menerima *invite* rapat ± 15 menit sebelum dimulai.
3) Pastikan sistem operasi resmi dan legal yg sudah terinstal di perangkat yang digunakan.
4) Pastikan perangkat yang digunakan sudah terpasang antivirus dan *firewall* yang diperbaharui secara berkala.
5) Pastikan akun yang digunakan adalah akun resmi dinas atau akun milik pribadi, bukan milik orang lain.
6) Pastikan nama *profile* sesuai dengan ketentuan yang disepakati sehingga mempermudah untuk melakukan kontrol terhadap partisipan yang tergabung. (mis: NAMA_INSTANSI).
7) Pastikan untuk berkoordinasi dengan *Host* apakah terdapat beberapa pengaturan dan konfigurasi yang harus dilakukan terhadap sistem operasi dan aplikasi *VC.*
8) Laksanakan kegiatan *VC* di tempat/ ruangan yang kondusif.
9) Tidak mengunggah tangkapan layar (*screenshot*) *VC* yang menampilkan ID rapat password, nama peserta, email atau informasi yang dianggap terbatas lainnya ke ruang bebas/publik seperti Internet.
10) Selalu melakukan evaluasi keamanan yang telah dilakukan demi mendapatkan hasil rapat bersama yang aman dan nyaman bagi semua.

c. Jaringan Internet:

1) Pastikan menggunakan jaringan internet pribadi atau jaringan internet yang terpercaya (*trusted*).
2) Agar tidak menggunakan jaringan internet untuk publik atau yang terpasang di tempat-tempat umum, seperti cafe, mal, atau restoran.
3) Sangat disarankan untuk menggunakan jaringan yang sudah dilengkapi dengan perangkat atau aplikasi *Virtual Private Network* (VPN) resmi.
4) Pastikan *bandwidth* cukup selama *VC* berlangsung.
5) Siapkan rencana komunikasi cadangan jika terjadi permasalahan, misalnya meminta partisipan untuk tetap terhubung melalui *tools* lainnya yang disepakati.

B. LANGKAH LANGKAH PENGAMANAN

1. **Prioritaskan keamanan jaringan**
   End point dan *platform VC* sering membutuhkan *Session Boarder Controller* (SBC) untuk mengatur traffic, termasuk mencari dan memblok koneksi mencurigakan. Pastikan aplikasi yang digunakan memiliki fitur SBC ini, selanjutnya lakukan pengaturan jaringan perlu di-*review* secara teratur untuk memastikan selalu *up to date*.
2. **Pentingnya penggunaan enkripsi**
   Bersama dengan keamanan jaringan, enkripsi merupakan hal yang mutlak bagi *VC*. Algoritma standar untuk *video conference* saat ini adalah AES 128 bit. Pastikan aplikasi yang digunakan minimal telah memiliki fitur enkripsi tersebut.
3. **Lindungi diri dengan "*Permission*"**
   Tidak semua kebocoran data terjadi karena *hacker/cracker* yang masuk kedalam sistem. Masalah keamanan dapat terjadi jika ada orang yang tidak berkepentingan dengan secara tidak sengaja diberi akses komunikasi yang seharusnya tidak dilihat misalnya karena tidak mendapatkan pengaturan yang benar. Oleh karenanya pastikan setiap peserta rapat yang diundang mendapatkan *permission* yang dikirim melalui jalur yang aman.
4. **Buat dan patuhi kebijakan untuk *VC***
   Jaringan yang aman dan enkripsi tidak akan berdampak besar pada keamanan *VC,* jika SDM yang menggunakan tidak memahami budaya keamanan. Kesalahan manusia (*human error*) merupakan penyebab terbesar terjadinya kebocoran data. Untuk itu perlu dibuat kebijakan/*policy* yang diantaranya mengatur bagaimana menggunakan sistem, bagaimana menggunakan perangkat mobile dan *remote* secara aman, hingga informasi apa saja yang dapat disampaikan pada saat *teleworking,*

C. *BEST PRACTICES*

1. Sebelum rapat:

1. Ketika menggunakan peralatan atau lokasi yang tidak biasa, lakukan pengujian koneksi sebelum rapat.
2. Jika mungkin, buat koneksi *VC* beberapa menit sebelum mulai rapat.
3. Pastikan setiap peserta rapat telah mendapatkan *permission* untuk bergabung pada *VC*.
4. Buat rencana komunikasi cadangan jika terjadi permasalahan koneksi, misalnya meminta peserta/ partisipan untuk tetap terhubung melalui laptop, menggunakan *mobile* atau *speakerphone*, dan/atau berkolaborasi melalui *tool* kolaborasi *online*.
5. Pastikan persyaratan keamanan telah terpenuhi seperti yang dijelaskan sebelumnya.

2. Selama rapat berlangsung:

1. Minta semua peserta membagikan tampilan video dan audio.
2. Minta peserta mematikan *microphone* jika lokasinya memiliki *noise* atau jika tidak sedang berbicara.
3. Diperlukan fasilitator rapat yang akan menyampaikan agenda rapat dan mengatur jalannya rapat.
4. Pastikan semua peserta memperoleh akses yang sama terhadap konten yang dibagikan selama *VC* dan menggunakan *tools* online jika mungkin.
5. Batasi penggunaan berbagi layar (*share desktop*), pastikan fitur berbagi layar dapat dikontrol oleh admin/ *Host*. Hal ini bertujuan untuk menghindari adanya peserta rapat yang berbagi layar yang tidak diinginkan.

Referensi: https://bssn.go.id (diakses 10 April 2020) diolah

II. MANUAL PRAKTIS PENGGUNAAN TINGKAT LANJUT DENGAN LISENSI AKUN BERBAYAR

Berikut adalah Manual Praktis Penyiapan dan Penyelenggaraan *VC*, dari *lesson learned VC* instansi lain. Manual Praktis disiapkan oleh Asdep Teleuti dengan penyesuaian lisensi akun Zoom di lingkup Deputi VI.

1. Teknis Penyiapan Undangan *VC*

1. Untuk pertemuan internal atau jumlah undangan di antara 15-20 orang
   (a) Berikan informasi kepada undangan mengenai ketentuan nama *profile* untuk mengikuti VC.
   (b) ID rapat dan *password* didistribusikan secara aman kepada partisipan undangan dengan melakukan *invite* lewat email/ media yang terpercaya, tidak secara publik (min 20 menit sebelum rapat dimulai).

2. Untuk pertemuan eksternal atau jumlah undangan di atas 20 orang
   (a) Sertakan tautan untuk registrasi *VC* dalam undangan.
   (b) Sebelum rapat berlangsung, partisipan harus melakukan registrasi dan konfirmasi kehadiran *VC* untuk dikirimkan undangan elektronik via *e-mail* yang berisikan ID rapat dan *password*. Teknis registrasi dan konfirmasi dapat dilakukan dengan aplikasi Zoom **(lihat Manual Praktis 2).**

2. Teknis Penyelenggaraan *VC*

1. *Host* (Asdep) mengatur *Meeting settings* **(lihat Manual Praktis 1).**
2. Jika ada bahan narasumber lain yang ingin ditampilkan saat *VC*, kirimkan sebelumnya kepada staf yang bertanggung jawab. Staf tersebut akan ditunjuk oleh *host* untuk menjadi *co-host* dalam membantu untuk menampilkan bahan dan menyetujui partisipan untuk bergabung dengan *VC* (cara menunjuk *co-host* lihat tautan halaman berikutnya).
3. *Co-host* disarankan terdiri dari minimal 2 orang atau lebih, dengan koneksi internet cepat untuk melakukan monitoring sepanjang *VC*.
4. Lakukan monitoring dan verifikasi terhadap setiap partisipan yang telah dan akan bergabung pada VC sesuai ketentuan yang yang disepakati (mis: NAMA_INSTANSI). Jika nama *profile* tidak sesuai dengan ketentuan, tidak akan diijinkan masuk ke dalam VC dari *waiting list*.
5. Jika ada partisipan yang mengganggu atau membuat keributan, *host* dan *co-host* dapat melakukan *mute audio* dan *video*, atau mengeluarkan partisipan dari *VC*.

3. Catatan

1. Manual Praktis akan terus diperbarui menyesuaikan kondisi kerja Deputi VI dan update terbaru aplikasi Zoom.
2. Jika ada pertanyaan, masukan, dan saran terkait dengan manual praktis bisa disampaikan ke:azwarcharis@gmail.com atau nugroho.sihombing@gmail.com

MENU: *SETTINGS-MEETING*	PENGATURAN	ACUAN PADA MANUAL/ KETERANGAN
Host Video	ON	C-2-1
Participants video	ON	C-2-1
Join before host	OFF	
Use Personal Meeting ID (PMI) when scheduling a meeting	OFF	A-2-a-(4)
Use Personal Meeting ID (PMI) when starting an instant meeting	OFF	A-2-a-(4)
Only authenticated users can join meetings from Web client	ON	A-2-a-(3)
Require password for participants joining by phone	ON	A-2-a-(4)
Chat	OFF	
File transfer	OFF	
Co-host	ON	Membantu Asdep untuk terima partisipan atau membagi layar
Screen sharing	ON	A-2-b-(9)
Who can share?	Host Only	A-2-b-(9)
Who can start sharing when someone else is sharing?	Host Only	A-2-b-(9)
Allow removed participants to rejoin	OFF	
Allow participants to rename themselves	OFF	
Waiting room *Choose which participants to place in the waiting room:* ***All participants***	ON	

Cara menunjuk *co-host*
https://support.zoom.us/hc/en-us/articles/206330935-Enabling-and-adding-a-co-host

MANUAL PRAKTIS 2—PENGGUNAAN FITUR REGISTRATION

Langkah-langkah untuk mengaktifkan fitur *registration* adalah sebagai berikut

A. Pengaturan *Schedule Meeting*

1. Atur *Topic* dan *Description Meeting*
2. Atur waktu, durasi, dan zona waktu
3. Atur *Registration* menjadi *required* (dicentang)
4. Atur *Meeting ID Generate Automatically*
5. Atur *Meeting Password Require meeting password* (dicentang)
6. Atur Video baik *Host* dan *Participant* dalam opsi ON
7. Atur *Meeting Options Mute participants upon entry* (dicentang), *Enable waiting room* (dicentang), *Only authenticated users can join: Sign in to Zoom* (dicentang)
8. Opsi lainnya yang tidak disebutkan di sini, tetap dalam keadaan semula (*default*) kemudian tekan *Save*.

B. Penyiapan Undangan Rapat

1. Setelah pengaturan *Schedule Meeting* selesai, akan muncul kolom
   Invite Attendees: People are required to register before joining this meeting.
   Registration URL: https://us02web.zoom.us/meeting/register/tZUqf-gvpzMvGtVRJhk6MjGDN1NRFZIsi6ge (contoh)
2. Tautan diatas yang bisa diperpendek dengan *link shortener*, kemudian dituliskan di undangan yang akan disebar. Penerima undangan harus mendaftarkan diri lewat tautan di atas, untuk mendapatkan tautan ID rapat dan *password*.
3. *Host* bisa mengatur *Registration Option* di bagian bawah halaman sebagai berikut

TAB REGISTRATION	
Approval	***Manually Approve*** *The organizer must approve registrants before they receive information on how to join the meeting.*
Notification	*Send an email to host when someone registers* (OFF)
Other options	*Close registration after event date* (DICENTANG) *Show social share buttons on registration page* (OFF)
TAB QUESTION	
	1. Tambahkan *Organization dan Job Title* (REQUIRED) sebagai pertanyaan pengaman

C. Persiapan Sebelum Rapat

1. *Host* bisa melakukan pengecekan pada partisipan yang sudah mendaftar di *Tab Pending Approval*, dengan melihat jawaban yang disampaikan, kemudian menekan *Approve*.
2. Terhadap list partisipan yang telah disetujui, akan dikirimkan email yang berisi tautan ID rapat (Click Here to Join) dan *password* secara otomatis.
3. Tautan pendaftaran diri akan ditutup setelah *VC* dimulai.

III. LAMPIRAN CONTOH DARI SINGAPORE DIGITAL (SG:D)