KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 3 TAHUN 2022

GARIS PANDUAN PENGURUSAN KESELAMATAN PENGGUNAAN PERSIDANGAN VIDEO (*VIDEO CONFERENCING*) DALAM PERKHIDMATAN AWAM

JABATAN PERDANA MENTERI

9 Disember 2022

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI
PRIME MINISTER'S DEPARTMENT
Blok B8, Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
MALAYSIA

Tel. : 03-8000 8000
Fax : 03-8888 3904
Web : http://www.jpm.gov.my
Emel : jpm@jpm.gov.my

Rujukan Kami: KPKK(R) 600-1/1 JLD.4 (14)

Tarikh: 9 Disember 2022

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

SURAT PEKELILING AM BILANGAN 3 TAHUN 2022

GARIS PANDUAN PENGURUSAN KESELAMATAN PENGGUNAAN PERSIDANGAN VIDEO (*VIDEO CONFERENCING*) DALAM PERKHIDMATAN AWAM

1. TUJUAN

Garis panduan ini bertujuan sebagai rujukan dan panduan kepada Jabatan mengenai pengurusan keselamatan perlindungan berhubung perkara rasmi dan rahsia rasmi Jabatan dalam penggunaan persidangan video (*video conferencing*).

2. LATAR BELAKANG

Perkembangan Revolusi Industri Keempat (IR4.0) memberikan kesan secara langsung kepada pelbagai bidang seperti yang dinyatakan dalam Rangka Kerja Tindakan Ekonomi Digital Malaysia (MyDigital). Revolusi ini memberi impak ekonomi digital sangat luas membabitkan masyarakat, perniagaan dan Kerajaan.

Bagi merealisasikan aspirasi Kerajaan Digital yang mampan, persidangan video menjadi alternatif kepada pegawai awam dan Jabatan dalam meningkatkan sistem penyampaian perkhidmatan awam yang cekap dan berkesan.

Di dalam Jabatan, persidangan video ini kini banyak digunakan bagi tujuan mesyuarat, perbincangan, latihan dan perkongsian maklumat. Ini termasuklah mengendalikan mesyuarat yang membincangkan perkara rahsia rasmi dan sensitif. Justeru itu, ia boleh memberi ancaman baharu seperti ketirisan maklumat yang mempunyai implikasi keselamatan kepada Jabatan sekiranya tiada kawalan yang sewajarnya diambil.

3. PELAKSANAAN

Garis Panduan Pengurusan Keselamatan Penggunaan Persidangan Video (*Video Conferencing)* Dalam Perkhidmatan Awam dilampirkan bersama surat pekeliling ini untuk rujukan dan pelaksanaan semua Jabatan.

4. PERANAN DAN TANGGUNGJAWAB KETUA JABATAN

Ketua Jabatan perlu mengambil langkah-langkah keselamatan sebelum, semasa dan selepas mengendalikan persidangan video agar maklumat rasmi dan rahsia rasmi tidak terdedah kepada pihak yang tidak dibenarkan semasa persidangan video berlangsung. Langkah-langkah keselamatan yang diambil hendaklah berdasarkan peruntukan-peruntukan yang dibenarkan oleh Kerajaan selari dengan kehendak undang-undang dan peraturan yang sedang berkuat kuasa.

5. KHIDMAT NASIHAT

Sebarang pertanyaan berkaitan dengan Surat Pekeliling ini boleh dikemukakan kepada:

Ketua Pegawai Keselamatan Kerajaan,
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia,
Jabatan Perdana Menteri,
Aras -1,1 dan 2, Setia Perdana 7 ,
Kompleks Setia Perdana,
Pusat Pentadbiran Kerajaan Persekutuan,
62502 PUTRAJAYA.

Telefon : 03-8872 6038 / 6039
Faks : 03- 8888 3258
E-mel : kictrr@cgso.gov.my

6. PEMAKAIAN

Surat Pekeliling Am ini terpakai kepada semua agensi Perkhidmatan Awam Persekutuan bermula dari tarikh pekeliling ini ditandatangani. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Surat Pekeliling Am ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Negeri dan Pihak Berkuasa Tempatan.

7. TARIKH KUAT KUASA

Surat Pekeliling ini berkuat kuasa mulai tarikh surat ini dikeluarkan.

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

(TAN SRI DATO' SERI MOHD ZUKI BIN ALI)
Ketua Setiausaha Negara

Lampiran kepada Surat Pekeliling Am Bilangan 3 Tahun 2022

KERAJAAN MALAYSIA

GARIS PANDUAN
PENGURUSAN KESELAMATAN PENGGUNAAN PERSIDANGAN VIDEO (*VIDEO CONFERENCING*) DALAM PERKHIDMATAN AWAM

PEJABAT KETUA PEGAWAI KESELAMATAN
KERAJAAN MALAYSIA

KANDUNGAN

TAFSIRAN

Tafsiran yang digunakan dalam garis panduan ini perlu difahami seperti berikut, melainkan jika konteksnya menghendaki makna yang lain:

a. **Ancaman** ertinya penyebab bagi insiden-insiden tidak diingini yang boleh mengakibatkan kemudaratan kepada Jabatan;

b. **Individu Dibenarkan *(Authorised Person)*** ertinya individu yang dibenarkan untuk mewujud, mengemaskini, menyimpan, mencetak atau menghantar maklumat Rahsia Rasmi;

c. **Integriti** ertinya jaminan ke atas kesahihan maklumat bahawa ianya tidak dipinda oleh entiti yang tidak sah;

d. **Jabatan** ertinya sesebuah Kementerian, Jabatan Kerajaan, Badan Berkanun, Kerajaan Tempatan dan agensi lain yang kepadanya Akta 88 terpakai;

e. **Kerahsiaan** ertinya jaminan bahawa maklumat tidak didedahkan kepada entiti yang tidak sah;

f. **Kerajaan** ertinya Kerajaan Malaysia;

g. **Keselamatan maklumat** ertinya perlindungan terhadap aspek kerahsiaan, integriti, ketersediaan dan ketidaksangkalan maklumat;

h. **Ketersediaan** ertinya keadaan yang mana maklumat boleh diperolehi dan digunakan apabila diperlukan oleh entiti yang dibenarkan;

i. **Ketirisan Maklumat** ertinya kebocoran atau kehilangan sesuatu data, berita atau laporan Jabatan yang dianggap sulit dari sumbernya. Ketirisan maklumat boleh berlaku sama ada dengan sengaja atau tidak disengajakan;

j. **Kriptografi** ertinya satu teknik keselamatan maklumat yang melibatkan pertukaran maklumat kepada format yang tidak difahami, yang dinamakan Teks Sifer. Teknik ini dilakukan menerusi penyulitan dengan menggunakan kekunci khas, manakala penyahsulitan adalah dengan menukarkan semula Teks Sifer kepada format asal;

k. **Maklumat Rasmi** ertinya maklumat yang ditafsirkan seperti di dalam Arahan Keselamatan (Semakan dan Pindaan 2017);

l. **Peranti Dibenarkan *(Authorised Device)*** ertinya sebarang peranti ICT yang berupaya menyimpan data yang dibekalkan oleh Jabatan kepada penjawat awam;

m. **Perkhidmatan Awam** ertinya perkhidmatan awam yang diliputi oleh Akta 88;

n. **Rahsia Rasmi** ertinya apa-apa suratan yang dinyatakan dalam Jadual dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa suratan rasmi, maklumat dan bahan lain sebagaimana yang boleh dikelaskan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad” mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu Negeri atau mana-mana pegawai awam yang dilantik di bawah seksyen 2B, Akta Rahsia Rasmi 1972 [*Akta 88*]; dan

o. **Serangan atau Ancaman Siber** ertinya suatu perbuatan di dalam atau di luar Malaysia terhadap maklumat, sistem komputer dan komunikasi, program komputer dan data yang dirancang atau bertujuan untuk mengendalakan, mengganggu secara serius, merosakkan atau memusnahkan apa-apa sistem komputer atau perkhidmatan komunikasi, perbankan atau kewangan, utiliti, pengangkutan atau infrastruktur penting yang lain dan termasuklah aktiviti jenayah terancang.

GARIS PANDUAN PENGURUSAN KESELAMATAN PENGGUNAAN PERSIDANGAN VIDEO (*VIDEO CONFERENCING*) DALAM PERKHIDMATAN AWAM

1. PENGENALAN

1.1. TUJUAN

Garis Panduan Pengurusan Keselamatan Penggunaan Persidangan Video (*Video Conferencing*) Dalam Perkhidmatan Awam bertujuan sebagai panduan kepada Jabatan mengenai pengurusan keselamatan perlindungan berhubung perkara rasmi dan rahsia rasmi Jabatan dalam penggunaan persidangan video (*video conferencing*).

1.2. LATAR BELAKANG

a. Persidangan video menjadi alternatif kepada pegawai awam dan Jabatan ke arah merealisasikan Kerajaan Digital bagi meningkatkan sistem penyampaian perkhidmatan. Sistem penyampaian ini boleh dilaksanakan menerusi pelbagai medium dan saluran komunikasi seperti penggunaan aplikasi dalam talian sama ada menggunakan aplikasi dalaman atau komersial; dan

b. Di dalam Jabatan, persidangan video ini kini banyak digunakan bagi tujuan mesyuarat, perbincangan, latihan dan perkongsian maklumat. Ini termasuklah mengendalikan mesyuarat yang membincangkan perkara rahsia rasmi dan sensitif. Justeru itu, ia boleh memberi ancaman baharu seperti ketirisan maklumat yang mempunyai implikasi keselamatan kepada Jabatan sekiranya tiada kawalan yang sewajarnya diambil.

2. OBJEKTIF

a. Menjelaskan kepentingan untuk melindungi maklumat Rahsia Rasmi yang diuruskan melalui persidangan video selaras dengan keperluan Arahan Keselamatan (Semakan dan Pindaan 2017); dan

b. Menerangkan langkah-langkah kawalan mitigasi yang wajar dan efektif berhubung risiko dan ancaman keselamatan berkaitan dengan persidangan video.

3. KEPERLUAN PERUNDANGAN DAN PERATURAN PERSIDANGAN VIDEO

a. Jabatan hendaklah mematuhi peraturan-peraturan pengurusan Rahsia Rasmi selaras dengan peruntukan-peruntukan yang terkandung dalam Akta Rahsia Rasmi 1972 [*Akta 88*] dan mematuhi perenggan 134, Arahan Keselamatan (Semakan dan Pindaan 2017) seperti berikut;

"Semua hubungan komunikasi jabatan seperti e-mel rasmi, pesanan segera (instant messaging), persidangan web (web conferencing, perkongsian sumber (shared resources), rangkaian tanpa-wayar (wireless) dan seumpamanya perlu dilindungi daripada capaian yang tidak dibenarkan."...".

b. Maklumat atau perkara rahsia rasmi yang dikendalikan melalui pelaksanaan atau perkhidmatan persidangan video perlu bebas daripada sebarang risiko dan ancaman seperti serangan perisian hasad, curi dengar (*eavesdropping*), *distributed-denial-of-services* (DDOS), penggodam dan lain-lain.

4. RISIKO KESELAMATAN PENGGUNAAN PERSIDANGAN VIDEO

Penggunaan persidangan video boleh mengundang pelbagai ancaman yang menjejaskan keselamatan individu dan organisasi. Antara ancaman dan kelemahan keselamatan yang dikenal pasti adalah seperti berikut:

4.1. KAWALAN KESELAMATAN FIZIKAL YANG LEMAH

a. Pengguna boleh menggunakan pelbagai peranti mudah alih seperti komputer riba, telefon pintar dan tablet termasuklah penggunaan peralatan persendirian (*Bring Your Own Devices-BYOD*) untuk mengakses persidangan video dari pelbagai lokasi seperti di rumah, kafeteria atau hotel. Peranti mudah alih ini terdedah kepada ancaman kecurian dan kehilangan yang menyebabkan maklumat di dalamnya dikompromi atau peranti tersebut digunakan sebagai akses kepada persidangan video; dan

b. Keselamatan fizikal bagi ruang dan tempat persidangan video juga tidak diperkukuhkan seperti terdedah kepada penglihatan umum atau perbualan yang mudah dicuri dengar.

4.2. RANGKAIAN TIDAK SELAMAT

Persidangan video membenarkan pengguna untuk akses perkhidmatan tersebut tanpa melalui rangkaian Jabatan seperti penggunaan jalur lebar persendirian, rangkaian tanpa wayar atau rangkaian selular. Rangkaian ini mungkin tidak selamat serta terdedah kepada risiko curi dengar (*eavesdropping*) dan komunikasi tersebut boleh diubahsuai.

4.3. KELEMAHAN KONFIGURASI PERANTI

Peralatan ICT yang digunakan untuk persidangan video tidak menjalani proses konfigurasi yang bersesuaian dengan keperluan keselamatan. Ini termasuklah

menggunakan *default setting* ke atas perkakasan dan perisian persidangan video serta tidak dikemas kini dengan *patches* terkini. Sebagai contoh penggunaan peranti seperti komputer riba yang terdedah dengan perisian hasad boleh mengakibatkan akses rangkaian termasuk sesi persidangan video dikompromi.

4.4. KEPELBAGAIAN APLIKASI PERSIDANGAN VIDEO

Persidangan video dilaksanakan melalui aplikasi yang dibangunkan oleh pihak penyedia luar dalam pelbagai platform sama ada yang dihoskan secara *cloud* atau dikonfigurasi dalam premis Jabatan. Penggunaan aplikasi persidangan video yang tidak terkawal dan tiada penilaian keselamatan boleh menyebabkan ancaman keselamatan terhadap maklumat Jabatan.

5. KESELAMATAN INFRASTRUKTUR PERSIDANGAN VIDEO

Secara asasnya keselamatan infrastruktur persidangan video terbahagi kepada komponen utama seperti berikut:

5.1. KESELAMATAN RANGKAIAN

a. Setiap persidangan video hendaklah disokong dengan infrastruktur rangkaian yang stabil dan selamat bagi mengelakkan sebarang gangguan dan pencerobohan keselamatan;

b. Jabatan hendaklah memastikan akses ke rangkaian persidangan video dilindungi dengan kawalan standard keselamatan seperti menggunakan saluran komunikasi selamat (HTTPS, SFTP, VPN yang menggunakan SSL atau IPSec dan TLS); dan

c. Selain itu, mekanisme perlindungan disokong dengan sistem pemantauan dan pengesanan aktif seperti *Intrusion & Prevention Detection System*

(IPDS) bagi memantau trafik rangkaian dan aktiviti hos sepanjang persidangan video tersebut berlangsung.

5.2. KESELAMATAN SISTEM DAN APLIKASI

a. Bagi urusan Rahsia Rasmi, Jabatan hendaklah memastikan aplikasi atau perkhidmatan persidangan video yang digunakan mempunyai ciri-ciri keselamatan yang boleh menyokong keperluan mandatori keselamatan seperti penggunaan Produk Kriptografi Terpercaya (PKT). Ini bagi memastikan kerahsiaan dan integriti maklumat rahsia rasmi dilindungi melalui penggunaan produk kriptografi yang telah dinilai dan disahkan oleh pihak Kerajaan;

b. Jabatan hendaklah menyediakan peraturan *accessibility* seperti menetapkan proses pengenalan (*authentication*) dan hak capaian pengguna kepada pentadbir sistem dan pelanggan/pengguna *(end-user)*;

c. Jabatan hanya boleh memilih penyedia perkhidmatan luar jika persidangan video menepati objektif keselamatan serta mematuhi peraturan dan langkah-langkah kawalan seperti yang digariskan di dalam dokumen ini;

d. Jabatan boleh menyediakan senarai aplikasi atau perkhidmatan persidangan video yang telah diperakukan tahap keselamatannya. Prosedur Kawalan Standard (SOP) ringkas pengendalian aplikasi atau sistem persidangan video turut dinyatakan sebagai panduan dan rujukan kepada kakitangan yang akan menggunakan perkhidmatan tersebut; dan

e. Penggunaan aplikasi persidangan video yang sentiasa dikemas kini dengan fungsi dan ciri-ciri keselamatan yang baharu dapat mengekang daripada ancaman keselamatan disebabkan oleh perisian yang usang (*obsolete*).

5.3. KESELAMATAN PERANTI DAN PERKAKASAN

a. Peranti pengguna boleh dibahagikan kepada 2 kategori iaitu:

i. **Komputer Peribadi (PC)** sama ada desktop atau komputer riba yang disokong dengan sistem pengoperasian (OS) seperti Windows, Apple OS X dan Linux; atau

ii. **Peranti Mudah Alih** seperti telefon pintar atau tablet yang disokong dengan sistem pengoperasian (OS) *mobile* seperti Apple iOS dan Google Android.

b. Jurang perbezaan di antara komputer peribadi dan peranti mudah alih semakin kecil. Peranti mudah alih pada waktu kini mempunyai lebih banyak fungsi berbanding dengan komputer peribadi. Begitu pun, tahap kawalan keselamatan ke atas peralatan ini sedikit berbeza yang perlu diberi perhatian oleh Jabatan khususnya apabila membuat pertimbangan risiko keselamatan bagi tujuan *remote access* atau persidangan video;

c. Pertimbangan risiko ini adalah berdasarkan kepada pihak-pihak yang bertanggungjawab terhadap kawalan keselamatan pada peralatan tersebut. Berikut merupakan perincian terhadap isu kawalan dan risiko keselamatan peranti pengguna mengikut kategori di bawah:

i. **Organisasi/Jabatan.** Peranti pengguna ini adalah hak milik Jabatan yang diperoleh, dikonfigurasi, di selenggara dan diuruskan oleh Jabatan untuk dibekalkan kepada pegawai awam;

ii. **Kawalan Pihak Ketiga**. Peranti pengguna ini dibekalkan dan dikawal selia oleh pihak lain seperti pihak kontraktor atau vendor. Pihak tersebut bertanggungjawab untuk melaksanakan langkah-langkah kawalan seperti menjalankan proses kemas kini sistem

pengoperasian, antivirus serta penyelenggaraan perisian dan perkakasan sepertimana yang termaktub dalam kontrak; dan

iii. ***Bring-Your-Own-Device (BYOD)*.** Peranti pengguna adalah hak milik dan dikawal sendiri oleh kakitangan Jabatan. Pengguna bertanggungjawab sepenuhnya terhadap kawalan dan konfigurasi keselamatan.

6. PELAKSANAAN PERSIDANGAN VIDEO BAGI MAKLUMAT RAHSIA RASMI

6.1. TANGGUNGJAWAB JABATAN / URUS SETIA

a. Jabatan hendaklah memastikan pengguna hanya menggunakan perisian persidangan yang disediakan atau yang telah diperakukan oleh pihak Jabatan sahaja;

b. Urus setia hendaklah menggunakan fungsi-fungsi keselamatan aplikasi persidangan video mengikut SOP atau manual sistem seperti yang telah ditetapkan;

c. Semua perkhidmatan persidangan video yang menguruskan **Rahsia Rasmi** hendaklah dihadkan kepada mereka yang boleh akses dengan menggunakan **Peranti Dibenarkan *(Authorised Device)*** sahaja;

d. Peranti dan perkakasan persidangan video hendaklah dipasang di tempat selamat seperti di dalam bilik yang mempunyai kawalan kunci dan akses yang bersesuaian dan telah dinilai tahap keselamatannya. Lokasi tersebut juga tidak terdedah kepada pendengaran dan penglihatan umum; dan

e. Sekiranya capaian persidangan video tersebut dibenarkan secara *remote access*, Jabatan hendaklah memastikan perkhidmatan tersebut mempunyai langkah-langkah kawalan keselamatan yang tertentu terlebih dahulu.

6.2. TANGGUNGJAWAB AHLI MESYUARAT / KAKITANGAN

a. Setiap ahli mesyuarat/kakitangan dilarang menggunakan akaun milik orang lain, menggunakan identiti palsu atau menyamar sebagai orang lain;

b. Bagi persidangan video yang dihoskan oleh pihak luar dan daripada sumber yang tidak diketahui, kakitangan hendaklah merujuk kepada Pegawai Keselamatan ICT (ICTSO) atau Pegawai Keselamatan Jabatan (PKJ) masing-masing untuk menilai kesesuaian menyertai persidangan video tersebut apabila ada Rahsia Rasmi dibincangkan;

c. Jika dibenarkan, kakitangan dinasihatkan untuk menyertai sesi persidangan video tersebut hanya melalui pelayan web *(browser)* tanpa perlu membuat sebarang pemasangan *client software* pada peranti pengguna;

d. Pemasangan perisian daripada sumber yang tidak diketahui boleh menyebabkan peranti dan maklumat pengguna terdedah kepada ancaman keselamatan;

e. Kakitangan Jabatan dilarang menggunakan e-mel rasmi untuk *sign-up* perisian percuma atau yang tidak sah;

f. Perkongsian dokumen rahsia rasmi atas talian adalah tidak dibenarkan. Jika terdapat keperluan, fail atau dokumen hanya boleh dikongsi atas kebenaran Ketua Jabatan sahaja;

g. Bahan-bahan rasmi yang hendak dimuat naik atau dikongsi hendaklah dibuat semakan terlebih dahulu dan mendapatkan pengesahan daripada pihak berkaitan;

h. Jika persidangan video secara *remote access* telah mendapat kebenaran daripada Ketua Jabatan, antara langkah-langkah kawalan fizikal dan

persekitaran ICT yang perlu diambil oleh kakitangan adalah seperti berikut:

i. memilih lokasi yang bersesuaian dan kurang berisiko atau di tempat yang telah dikhaskan. Tempat awam seperti lobi hotel, kafeteria, restoran, kafe siber atau kios awam adalah tidak dibenarkan;

ii. ruang kerja kakitangan tidak terdedah kepada penglihatan dan pendengaran umum;

iii. penggunaan perkakasan dan peranti peribadi **BYOD** seperti telefon pintar, komputer riba dan komputer desktop bagi persidangan video yang melibatkan **Rahsia Rasmi adalah DILARANG** sama sekali. Namun begitu, penggunaan BYOD untuk tujuan rasmi yang lain adalah berdasarkan polisi BYOD di agensi dan Kementerian masing-masing; dan

iv. kakitangan tidak meninggalkan perkakasan persidangan video (PC/Notebook) tanpa dikunci atau dibiarkan tanpa pengawasan apabila perlu meninggalkan sidang video semasa atau selepas sesi berlangsung.

7. TATACARA PELAKSANAAN PERSIDANGAN VIDEO

7.1. SEBELUM SIDANG VIDEO

a. E-mel atau surat jemputan yang mengandungi pautan (*link*) ke persidangan hendaklah dihantar kepada nama dan alamat yang dibenarkan sahaja seperti akaun e-mel rasmi Jabatan;

b. Maklumat login seperti nombor ID, *dialing number* dan kata laluan hendaklah dihantar berasingan. Kata laluan yang disediakan hendaklah kukuh dan mengikut amalan terbaik keselamatan;

c. Satu peringatan diberikan kepada pengguna untuk menjaga kerahsiaan maklumat seperti tidak berkongsi maklumat login kepada pihak lain dan mendedahkan pautan tersebut di platform awam seperti media sosial;

d. Pentadbir sistem dilarang mendaftar masuk persidangan video dengan menggunakan akaun admin yang mempunyai hak keistimewaan aplikasi *(administrative privileges)*;

e. Urus setia hendaklah mahir mengendalikan aplikasi sidang video. Satu sesi *dry-run* boleh dilaksanakan oleh pihak urus setia dengan sokongan teknikal ICT bagi menguji ketersediaan perkhidmatan. Kakitangan yang tidak mahir mengendalikan fungsi atau *features* tertentu boleh mengakibatkan pengoperasian persidangan video berada di luar kawalan; dan

f. Pengurusan perkongsian fail dan skrin serta rakaman yang betul boleh mengelakkan akses kepada maklumat sensitif daripada pihak yang tidak dibenarkan.

7.2. SEMASA SIDANG VIDEO

a. Sebelum memulakan sebarang persidangan video, satu nota peringatan keselamatan hendaklah diberikan kepada semua pengguna akan kepentingan untuk menjaga keselamatan maklumat;

b. Jika perlu, SOP dan manual ringkas pengendalian aplikasi sidang video juga boleh diberikan;

c. Paparan antara muka aplikasi persidangan video sebaik-baiknya mempunyai kod khas, nama dan agensi yang mewakili identiti pengguna;

d. Identiti pengguna penting kepada pihak urus setia bagi menentukan individu yang menyertai persidangan video adalah daripada pihak yang sah;

e. Pihak urus setia boleh mengeluarkan atau menamatkan sesi dari akaun atau identiti yang tidak boleh disahkan atau meragukan. Kebanyakan aplikasi persidangan video mempunyai kemudahan '*waiting room*' untuk membolehkan urus setia mengenal pasti individu sebelum akses ke persidangan video tersebut diberi;

f. Sekiranya ada keperluan, rakaman hanya boleh diaktifkan oleh pihak urus setia. Pihak urus setia hendaklah memastikan fungsi menyalin atau menawan rekod di peringkat pengguna dinyahaktifkan;

g. Pihak urus setia hendaklah memantau paparan skrin pengguna sepanjang masa dan mengambil tindakan pembetulan apabila ada paparan audio atau visual yang tidak berkaitan daripada pengguna; dan

h. Peranti dan perkakasan persidangan video yang telah dipasang tidak boleh dibiarkan tanpa pengawasan.

7.3. SELEPAS SIDANG VIDEO

a. Salinan rakaman hendaklah disimpan di dalam storan milik Jabatan seperti storan primer perkakasan dan peralatan persidangan video (*local drive*) atau fasiliti lain yang telah disahkan;

b. Jabatan perlu berhati-hati menggunakan kemudahan mod rakaman. Sistem pemprosesan dan penyimpanan data sama ada secara fizikal atau maya perlu diketahui dengan jelas bagi menentukan fungsi tersebut boleh diguna atau tidak. Sebagai contoh, maklumat rakaman disimpan dalam pengkomputeran awan yang telah dipilih secara *default* oleh penyedia aplikasi. Oleh itu, keselamatan pengkomputeran awan juga adalah perkara yang perlu dinilai pihak jabatan;

c. Salinan rakaman ini merupakan rekod Jabatan yang perlu dijamin keselamatannya. Rekod ini tidak boleh sesekali disalin, dikongsi atau diterbitkan tanpa kebenaran daripada pihak pemula atau Jabatan;

d. Elakkan penggunaan *shared folder* yang boleh diakses oleh banyak pihak atau memuat naik fail tersebut ke platform awam seperti Youtube, Facebook, Instagram, Google dan sebagainya; dan

e. Memastikan sesi persidangan video telah ditamatkan dengan betul dengan tidak meninggalkan apa-apa bahan pada paparan skrin secara atas talian atau pada perkakasan persidangan.

8. ETIKA PENGGUNAAN PERSIDANGAN VIDEO

Berikut merupakan etika baik yang perlu dipatuhi bagi setiap ahli mesyuarat apabila menggunakan persidangan video:

a. menyertai sesi persidangan video lebih awal atau sebelum sesi bermula;

b. memastikan kamera sentiasa diaktifkan, berfungsi dan memaparkan *live image* (wajah sebenar) sepanjang sesi persidangan video diadakan;

c. memastikan latar belakang skrin adalah bersesuaian dan tidak mengandungi imej atau perkataan yang sensitif;

d. mengenakan kod etika pakaian yang bersesuaian dengan persidangan video yang disertai;

e. mengelakkan sebarang situasi yang boleh mengganggu sesi persidangan video seperti membiarkan mikrofon dipasang apabila tidak diperlukan;

f. memilih lokasi yang terhindar daripada gangguan bunyi bising;

g. mengikuti persidangan video mengikut tempoh masa yang telah ditetapkan. Jika perlu meninggalkan persidangan video satu pemakluman kepada pihak urus setia hendaklah diberikan; dan

h. menggunakan ruang *'chat box'* atau fungsi lain sepertinya untuk mengemukakan pandangan atau pertanyaan. Elakkan mencelah dan mengaktifkan mikrofon sekiranya tiada keperluan untuk berbuat demikian.

9. INSIDEN PELANGGARAN

a. Sekiranya berlaku sebarang insiden pelanggaran keselamatan seperti kecurian, kehilangan, kebocoran dan sebagainya khususnya semasa pengendalian rahsia rasmi semasa persidangan video tersebut, Ketua Jabatan atau Pegawai Keselamatan Jabatan hendaklah menyiasat punca berlakunya insiden tersebut dan mengambil tindakan menurut perenggan 116 atau 140 Arahan Keselamatan (Semakan dan Pindaan 2017); dan

b. Ketua Jabatan hendaklah mengambil tindakan tatatertib ke atas sebarang kecuaian yang berlaku manakala laporan polis hendaklah dibuat sekiranya disyaki sesuatu kesalahan jenayah telah berlaku menurut perenggan 117 atau 141 Arahan Keselamatan (Semakan dan Pindaan 2017).

10. PENUTUP

Garis panduan ini mengandungi prosedur tindakan dan kawalan yang perlu diambil oleh Ketua Jabatan dan pegawai awam yang berkenaan apabila menguruskan dan menggunakan persidangan video agar maklumat rasmi dan rahsia rasmi tidak terdedah kepada sebarang bentuk ancaman keselamatan yang boleh menyusahkan pentadbiran Kerajaan, menjejaskan keselamatan dan kesejahteraan negara.