KETUA PENGARAH KESELAMATAN NEGARA
MAJLIS KESELAMATAN NEGARA
Jabatan Perdana Menteri
Aras LG & G Blok Barat
Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

Tel : 03 - 8872 4201
Faks : 03 - 8888 3001
Portal Rasmi : www.mkn.gov.my
E-mel : kpkn@mkn.gov.my

Ruj. Tuan :
Ruj. Kami : MKN.600-8/4/1(S) (2)
Tarikh : 20 Februari 2025

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

YBhg. Tan Sri/ Datuk Seri/ Dato' Seri/ Datuk/ Dato'/ Tuan/ Puan,

SURAT EDARAN GARIS PANDUAN KESELAMATAN SIBER BAGI PENGANJURAN MESYUARAT BERKAITAN KEPENGERUSIAN ASEAN 2025

Izinkan saya dengan segala hormatnya menjemput perhatian YBhg. Tan Sri/ Datuk Seri/ Dato' Seri/ Datuk/ Dato'/ tuan/ puan kepada perkara di atas.

2. Seperti YBhg. Tan Sri/ Datuk Seri/ Dato' Seri/ Datuk/ Dato'/ tuan/ puan sedia maklum, Malaysia secara rasminya mengambil alih kepengerusian ASEAN bermula 1 Januari 2025.

3. Sehubungan dengan itu, satu (1) garis panduan keselamatan siber telah dibangunkan oleh pihak NACSA bagi memastikan keselamatan siber terjamin semasa mesyuarat ASEAN dijalankan.

4. Sekiranya terdapat sebarang pertanyaan mengenai perkara ini, bolehlah menghubungi:

Agensi Keselamatan Siber Negara (NACSA)
Majlis Keselamatan Negara
Aras LG & G, Blok Barat
Bangunan Perdana Putra
62502 PUTRAJAYA
E-mel: admin@nacsa.gov.my

5. Sukacita bersama-sama ini dilampirkan garis panduan tersebut untuk rujukan YBhg. Tan Sri/ Datuk Seri/ Dato' Seri/ Datuk/ Dato'/ tuan/ puan selanjutnya jua.

Sekian, terima kasih dan salam hormat.

"MALAYSIA MADANI"
"BERKHIDMAT UNTUK NEGARA"
"KESELAMATAN NEGARA TANGGUNGJAWAB BERSAMA"

Saya yang menjalankan amanah,

(RAJA DATO' NUSHIRWAN BIN ZAINAL ABIDIN)

s.k.

YAB Dato' Seri Anwar bin Ibrahim
Perdana Menteri
Pejabat YAB Perdana Menteri
Aras 5, Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya.

YBhg. Tan Sri Shamsul Azri bin Abu Bakar
Ketua Setiausaha Negara
Jabatan Perdana Menteri
Aras 4, Blok Timur Bangunan Perdana Putra
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya.

GARIS PANDUAN KESELAMATAN SIBER BAGI PENGANJURAN MESYUARAT BERKAITAN KEPENGERUSIAN ASEAN 2025

1. TUJUAN

1.1. Garis panduan keselamatan siber ini bertujuan:

(i) menyediakan panduan kepada semua Kementerian, Jabatan, Agensi, serta pihak berkaitan yang terlibat dalam penganjuran mesyuarat sepanjang kepengerusian Malaysia dalam ASEAN 2025;

(ii) memastikan langkah-langkah keselamatan siber diterapkan sepanjang penganjuran mesyuarat, terutama bagi mesyuarat yang diadakan di luar premis Kerajaan; dan

(iii) menjamin kelancaran penganjuran mesyuarat tanpa gangguan atau ancaman terhadap keselamatan siber.

2. TAFSIRAN

2.1. Bagi tujuan Garis Panduan ini, beberapa terma ditafsirkan seperti berikut:

(i) **"Agensi"** ialah agensi sektor awam yang merangkumi kementerian dan jabatan pada peringkat pentadbiran Kerajaan, Kerajaan Persekutuan, Badan Berkanun Persekutuan, Pejabat Setiausaha Kerajaan (SUK) Negeri, Badan Berkanun Negeri serta Pihak Berkuasa Tempatan (PBT).

(ii) **"Ancaman keselamatan siber"** ertinya suatu perbuatan atau aktiviti yang dijalankan terhadap atau melalui suatu komputer atau sistem komputer, tanpa kuasa yang sah, yang boleh secara ketaranya membahayakan atau boleh menjejaskan keselamatan siber komputer atau sistem komputer itu atau komputer atau sistem komputer yang lain.

(iii) **"ASEAN"** atau Persatuan Negara-negara Asia Tenggara ialah sebuah organisasi serantau yang ditubuhkan pada 8 Ogos 1967. Negara-negara anggota ASEAN melibatkan Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Filipina, Singapura, Thailand dan Vietnam.

(iv) **“Dokumen”** adalah apa-apa jenis maklumat atau data yang tercatat berkenaan dengan perkara-perkara rasmi seperti yang dinyatakan dalam Arahan Keselamatan (Semakan dan Pindaan 2017).

(v) **“GSC”** atau Government Secure Communication ialah sistem komunikasi selamat yang digunakan oleh agensi kerajaan pada peranti telefon mudah alih bagi melindungi maklumat rahsia rasmi daripada ancaman keselamatan siber. Sistem ini memastikan keselamatan komunikasi rasmi seperti suara, data, dan mesej melalui enkripsi serta kawalan akses ketat, menjadikannya terlindung daripada pengintipan atau gangguan pihak tidak berautoriti. Penggunaan sistem GSC ini merangkumi aplikasi mudah alih Unified Endpoint Management (UEM) dan SecuSUITE, yang dibekalkan oleh **Majlis Keselamatan Negara (MKN)** kepada pegawai dari agensi berkaitan bagi memastikan keselamatan komunikasi dan pengurusan peranti.

(vi) **“Insiden keselamatan siber”** ertinya suatu perbuatan atau aktiviti yang dijalankan terhadap atau melalui suatu komputer atau sistem komputer, tanpa kuasa yang sah, yang membahayakan atau menjejaskan keselamatan siber komputer atau sistem komputer itu atau komputer atau sistem komputer yang lain.

(vii) **“Keselamatan siber”** ertinya keadaan yang dalamnya suatu komputer atau sistem komputer dilindungi daripada apa-apa serangan atau akses yang tidak dibenarkan, dan disebabkan oleh keadaan itu—

(a) komputer atau sistem komputer itu terus tersedia dan boleh dikendalikan;

(b) integriti komputer atau sistem komputer itu adalah terpelihara; dan

(c) integriti dan kerahsiaan maklumat yang disimpan dalam, diproses oleh atau dihantar melalui, komputer atau sistem komputer itu adalah terpelihara.

(viii) **“CSIRT Agensi”** ialah pasukan tindak balas insiden keselamatan siber yang merangkumi kementerian dan jabatan pada peringkat pentadbiran Kerajaan, Kerajaan Persekutuan, Badan Berkanun Persekutuan, Pejabat Setiausaha Kerajaan (SUK) Negeri, Badan Berkanun Negeri serta Pihak Berkuasa Tempatan (PBT).

(ix) **“Penilaian risiko”** adalah proses mengenal pasti, menganalisis dan menilai risiko. Ini biasanya dilakukan untuk menguruskan ketidakpastian dan mengelakkan potensi kerugian atau bahaya. Penilaian risiko membantu organisasi dan individu membuat keputusan yang lebih bijak dengan

mempertimbangkan kemungkinan kesan dan kebarangkalian sesuatu risiko berlaku.

(x) **"Peralatan ICT"** merangkumi sistem komputer peribadi, terminal, alat-alat *peripheral* komputer, perkakasan dan rangkaian komunikasi, perisian komputer, sistem aplikasi, perkakasan storan, kemudahan peralatan sokongan, bekalan kuasa atau seumpamanya.

(xi) ***"*Prinsip *Zero-Trust Security"*** adalah model keselamatan siber yang berpegang kepada prinsip "Jangan Percaya, Sentiasa Sahkan" (Never Trust, Always Verify). Ciri-ciri *Zero-Trust Security* adalah seperti berikut:

(a) **Pengesahan Berterusan (Continuous Verification)**

- Semua akses mesti disahkan setiap kali, tanpa mengira sama ada pengguna atau peranti telah berada dalam rangkaian sebelum ini.
- Pengesahan pelbagai faktor (Multi-Factor Authentication, MFA) digunakan untuk meningkatkan keselamatan siber.

(b) **Akses Minimum (Least Privilege Access)**

- Pengguna dan peranti hanya diberikan akses yang diperlukan untuk tugas tertentu sahaja.
- Akses tambahan hanya diberikan jika perlu dan dengan kebenaran.

(c) **Segmentasi Mikro (Micro-Segmentation)**

- Rangkaian dipecahkan kepada beberapa segmen kecil untuk menghadkan pergerakan lateral serangan siber.
- Jika berlaku pelanggaran keselamatan siber, kesannya dapat dikawal dalam satu segmen sahaja tanpa menjejaskan seluruh sistem.

(d) **Pemantauan Berterusan & Analitik (Continuous Monitoring & Analytics)**

- Aktiviti pengguna dan peranti dipantau secara berterusan untuk mengesan sebarang kelakuan yang mencurigakan.
- Penggunaan kecerdasan buatan (AI) dan analisis tingkah laku membantu mengenal pasti ancaman keselamatan siber yang mungkin berlaku.

(e) **Pendekatan Berasaskan Identiti (Identity-Centric Security)**

- Identiti pengguna dan peranti menjadi faktor utama dalam menentukan tahap akses dan kepercayaan.
- Teknologi seperti *Zero Trust Network Access* (ZTNA) menggantikan VPN tradisional untuk memastikan akses lebih selamat.

(f) **Enkripsi Data (Data Encryption)**

- Semua data yang dihantar dan disimpan mesti dienkrip untuk mengelakkan capaian tidak sah.
- Perlindungan ini melibatkan enkripsi hujung-ke-hujung (end-to-end encryption).

(g) **Automasi dan Respons Pantas**

- Penggunaan automasi dalam pengurusan keselamatan siber membolehkan respons lebih pantas terhadap ancaman keselamatan siber.
- Teknologi seperti *Security Information and Event Management* (SIEM) dan

Extended Detection and Response (XDR) membantu dalam pengesanan dan tindak balas ancaman keselamatan siber.

3. LATAR BELAKANG

3.1. Bermula 1 Januari 2025, Malaysia secara rasminya mengambil alih kepengerusian ASEAN daripada Laos dengan tema "Keterangkuman dan Kemampanan".

3.2. Tema “Keterangkuman dan Kemampanan” adalah bertunjangkan naratif Malaysia MADANI yang bermatlamat memperkasa rakyat melalui keadilan sosial dan ekonomi, dalam usaha memastikan kesejahteraan jangka panjang daripada semua aspek kehidupan.

3.3. Keutamaan Malaysia dalam kepengerusian kali ini adalah untuk mengukuhkan **kepusatan ASEAN,** membina kepercayaan strategik di kalangan negara melalui dialog yang berterusan, diplomasi dan kemuafakatan, mempromosi perdagangan dan pelaburan intra-ASEAN, serta memastikan elemen keterangkuman dan kemampanan menjadi fokus utama dalam usaha-usaha pembangunan komuniti serantau.

3.4. Dianggarkan lebih daripada 350 mesyuarat dijadualkan semasa Malaysia menjadi Pengerusi ASEAN 2025 termasuk penganjuran Sidang Kemuncak ASEAN ke-46 dan ke-47 yang akan dihadiri oleh pemimpin negara anggota ASEAN.

4. PROSEDUR KESELAMATAN SIBER BAGI PENGANJURAN MESYUARAT

4.1. Mesyuarat yang telah dijadualkan akan melibatkan kehadiran pemimpin negara, pegawai kanan dan pegawai-pegawai teknikal dari negara anggota ASEAN serta rakan dialog ASEAN. Antara perkara yang akan dibincangkan semasa mesyuarat berkenaan akan menyentuh pelbagai bidang termasuk pengukuhan kerjasama dalam bidang ekonomi, politik, keselamatan dan sosial dengan matlamat untuk memperkukuh kestabilan, kemakmuran, dan kesejahteraan serantau.

4.2. Bagi memastikan integriti, kerahsiaan dan ketersediaan maklumat sepanjang penganjuran mesyuarat adalah terpelihara dan teratur, setiap agensi Kerajaan yang bertindak sebagai urus setia mesyuarat ASEAN perlu mematuhi prosedur keselamatan siber seperti berikut:

(i) **Pelaksanaan Sebelum Mesyuarat**

(a) **Penilaian Risiko**

Menjalankan penilaian risiko untuk mengenal pasti kebarangkalian ancaman dan insiden keselamatan siber dengan mengambil kira aspek kerahsiaan, integriti dan ketersediaan dokumen dan perkhidmatan.

(b) **Kawalan Akses Dalam Talian**

Pastikan akses dalam talian hanya diberikan kepada pihak yang telah disahkan sahaja, mengikut prinsip *zero-trust security*.

(c) **Keselamatan Peralatan ICT**

Pastikan semua peralatan ICT yang digunakan semasa mesyuarat dilindungi dengan ciri-ciri keselamatan yang telah dikemaskini, perlindungan terhadap ancaman keselamatan siber dan virus, perlindungan peranti pengguna, perlindungan *firewall* dan rangkaian.

(ii) **Pelaksanaan Semasa Mesyuarat**

(a) **Saluran Komunikasi Selamat dan Stabil**

Gunakan saluran komunikasi yang mempunyai ciri keselamatan *end-to-end*

encryption dan saluran rangkaian melalui kaedah *network segmentation* atau menggunakan talian khusus. Sebarang komunikasi rasmi melalui peranti telefon mudah alih, termasuk panggilan suara, pemindahan data, dan mesej, hendaklah mengguna pakai sistem GSC.

(b) **Akses Terhad Kepada Dokumen (Akses, Kendali dan Simpan)**

Hadkan akses dan pengendalian dokumen kepada ahli mesyuarat dengan mengambil kira prinsip-prinsip berikut; Perlu Mengetahui, Perlu Menyimpan, Lihat dan Kembalikan bagi pengendalian maklumat dalam persekitaran ICT – Rujuk kepada **Arahan Keselamatan (Semakan dan Pindaan 2017) Bab 2(IV): Prinsip-prinsip keselamatan dan Bab 5 (VI): Pengendalian Maklumat dalam Persekitaran ICT.**

(c) **Storan Awan**

Penggunaan perkhidmatan pengkomputeran awan hendaklah mematuhi dan berpandukan kepada **Arahan Keselamatan (Semakan dan Pindaan 2017) Bab 5 (VI): Pengendalian Maklumat dalam Persekitaran ICT** dan **Surat Pekeliling Am**

Bilangan 2 Tahun 2021 versi 2.0 - Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam.

(d) **Pengurusan dan Pengendalian Insiden Keselamatan Siber**

Sekiranya berlaku sebarang insiden keselamatan siber, laporkan terus kepada Agensi Penganjur untuk tindakan Pasukan CSIRT Agensi – Rujuk kepada **Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022.**

(iii) **Pelaksanaan Selepas Mesyuarat**

(a) Semua peranan dan akses yang telah diberikan sebelum dan semasa mesyuarat hendaklah dibatal, dinyahpasang dan dinyahaktif selepas mesyuarat selesai; dan

(b) Melaksanakan pelupusan rekod dan dokumen digital berdasarkan **Dasar Pengurusan Rekod dan Arkib Elektronik yang dikeluarkan oleh Arkib Negara Malaysia.**

5. PEMAKAIAN

Garis panduan ini terpakai kepada semua kementerian, jabatan dan agensi yang melaksanakan mesyuarat berkaitan kepengerusian ASEAN 2025.

6. TARIKH KUAT KUASA

Garis panduan ini berkuat kuasa mulai tarikh kelulusan surat ini hingga 31 Disember 2025.

7. RUJUKAN

(i) Akta Keselamatan Siber 2024 (Akta 854).

(i) Arahan Keselamatan (Semakan dan Pindaan 2017).

(ii) Dasar Pengurusan Rekod dan Arkib Elektronik.

(iii) Pekeliling Am Bilangan 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022.

(iv) Surat Pekeliling Am Bilangan 2 Tahun 2021 versi 2.0 - Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (Cloud Computing) Dalam Perkhidmatan Awam.

(v) Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024.