JABATAN PERDANA MENTERI
AGENSI KESELAMATAN SIBER NEGARA

GARIS PANDUAN KESIAPSIAGAAN DAN PENGENDALIAN ANCAMAN KESELAMATAN SIBER

A. TUJUAN DAN PEMAKAIAN

Garis Panduan ini bertujuan sebagai rujukan untuk mempertingkat kesiapsiagaan, pengesanan awal, tindak balas ancaman dan kesinambungan perkhidmatan. Oleh itu, organisasi adalah dimohon untuk meningkatkan tahap kesiapsiagaan, pemantauan dan perlindungan terhadap sistem, maklumat dan kesinambungan perkhidmatan masing-masing sebagai langkah pencegahan dan bagi memperkukuh daya tahan keselamatan siber negara.

Pelaksanaan ini hendaklah mengambil kira tahap risiko, tahap kritikal sistem dan keperluan operasi. Pengujian dan perubahan terhadap sistem perlu dibuat secara teliti supaya tidak menjejaskan penyampaian perkhidmatan. Garis Panduan ini tidak mewujudkan suatu kewajipan perundangan yang baharu.

Garis Panduan ini merupakan dokumen dinamik (*living document*) yang akan disemak dan dikemas kini dari semasa ke semasa bagi mengambil kira perkembangan teknologi, landskap ancaman keselamatan siber, perubahan dasar serta keperluan pelaksanaan.

B. TINDAKAN KESIAPSIAGAAN DAN PENGENDALIAN ANCAMAN KESELAMATAN SIBER MENGIKUT TURUTAN KEUTAMAAN

Tindakan kesiapsiagaan dan pengendalian ancaman keselamatan siber disusun mengikut keutamaan seperti yang berikut:

1. Aktifkan Penyelarasan, Tetapkan Pegawai Bertanggungjawab dan Saluran Komunikasi
2. Kenal Pasti Tanda Kompromi dan Ancaman Aktif
3. Lindungi Akses dan Permukaan Serangan Siber (*Attack Surface*)
4. Semak Kerentanan dan Laksanakan Tampalan (Patch) Kritikal
5. Sahkan Sandaran dan Kebolehpulihan Data
6. Laksanakan Penilaian Kerentanan dan Ujian Penembusan (*Vulnerability Assessment and Penetration Testing* (*VAPT*)) Secara Bersasar
7. Perkukuh Kawalan Pembekal dan Hubungan dengan Pihak Ketiga

8. Kemas Kini/Laksanakan Penilaian Risiko, Pelan Respons Insiden dan Pelan Kesinambungan
9. Laksanakan Keselamatan Data dan Rangkaian Berkriptografi Penuh
10. Gunakan *Application Programming Interface* (*API*) Bertandatangan Digital
11. Laksanakan Inventori dan Audit Penggunaan Kriptografi
12. Lapor, Eskalasi dan Pantau Penutupan Tindakan

Tindakan Kesiapsiagaan di bawah Garis Panduan ini disusun mengikut keutamaan supaya dapat dilaksanakan oleh pasukan yang bertanggungjawab dan dipantau oleh pihak pengurusan organisasi.

1. Aktifkan Penyelarasan, Tetapkan Pegawai Bertanggungjawab dan Saluran Komunikasi

Komponen	Perincian
Tujuan	Memastikan semua pihak mengetahui siapa yang membuat keputusan dan siapa yang perlu dihubungi sekiranya berlaku gangguan.
Langkah pelaksanaan	1. Ketua Jabatan/ Pengurusan Tertinggi mengarahkan Pegawai Keselamatan ICT (ICTSO/CISO) menyelaras tindakan, serta memastikan Pasukan Tindak Balas Insiden Keselamatan Siber, CSIRT/ Pusat Operasi Keselamatan, SOC), pemilik sistem dan pembekal kritikal bersiap siaga. 2. Sediakan senarai sistem atau perkhidmatan paling kritikal, contohnya portal utama, sistem pembayaran atau sistem operasi penting. 3. Tetapkan dan sahkan nama dan nombor untuk dihubungi bagi pegawai pasukan ICT, pemilik sistem, pihak pengurusan dan pembekal penting.
Penyelaras	Ketua Jabatan / *Information Communication Technology Security Officer* (ICTSO) / *Chief Information Security Officer* (CISO)
Bukti pelaksanaan yang disarankan	Senarai nama dan nombor untuk dihubungi pegawai bertanggungjawab, senarai sistem kritikal serta rekod arahan/ prosedur berkaitan.

2. Kenal Pasti Tanda Kompromi dan Ancaman Aktif

Komponen	Perincian
Tujuan	Mengenal pasti tanda kompromi dan ancaman aktif lebih awal sebelum merebak dan menjejaskan operasi.
Langkah pelaksanaan	1. Semak amaran daripada SOC/SIEM, EDR, *firewall*, VPN, e-mel, sistem identiti dan log. 2. Utamakan cubaan log masuk gagal yang berulang, aktiviti luar biasa, pemindahan data yang tidak lazim, tanda *ransomware* dan perubahan konfigurasi tanpa kebenaran. 3. Dapatkan maklum balas pemilik sistem tentang sistem yang tiba-tiba perlahan, fail yang tidak boleh dibuka, mesej tebusan atau perubahan yang tidak dibenarkan. 4. Sekiranya terdapat petunjuk serangan, maklumkan pasukan tindak balas insiden dengan segera. Log dan bukti digital hendaklah dipelihara dan tidak dipadam.
Penyelaras	Pasukan keselamatan ICT / CSIRT / SOC / pemilik sistem
Bukti pelaksanaan yang disarankan	Log semakan, amaran, tindakan dan ringkasan status (tiada petunjuk/ perlu siasatan/ insiden disahkan).

3. Lindungi Akses dan Permukaan Serangan Siber (*Attack Surface*)

Komponen	Perincian
Tujuan	Memperkukuh perlindungan sistem daripada diakses tanpa kebenaran.
Langkah pelaksanaan	1. Memperkukuh kawalan akses, termasuk pengaktifan *Multi-Factor Authentication* (MFA), semakan akaun berkeistimewaan tinggi dan penamatan akses yang tidak diperlukan. 2. Semak akaun bekas kakitangan, akaun yang tidak digunakan dan akses vendor serta nyahaktif akses yang tidak lagi diperlukan.

Komponen	Perincian
	3. Semak perkhidmatan yang terdedah ke Internet termasuk konfigurasi VPN, *firewall* dan peraturan akses. 4. Setiap perubahan hendaklah direkodkan dan diluluskan. Elakkan perubahan tergesa-gesa yang boleh mengganggu sistem kritikal.
Penyelaras	Pasukan keselamatan ICT / pentadbir sistem / pemilik proses
Bukti pelaksanaan yang disarankan	Senarai akaun dan akses yang telah disemak, tindakan pembetulan dan rekod perubahan yang diluluskan.

4. Semak Kerentanan dan Laksanakan Tampalan (*Patch*) Kritikal

Komponen	Perincian
Tujuan	Menutup ruang kelemahan yang boleh dieksploitasi.
Langkah pelaksanaan	1. Utamakan kerentanan yang diketahui sedang dieksploitasi secara aktif, sistem yang terdedah ke Internet dan aset berimpak tinggi kepada operasi. 2. Laksanakan tampalan (*patch*) iaitu kemas kini bagi membaiki kelemahan. Bagi sistem *Operational Technology/Industrial Control System* (OT/ICS) dan sistem sensitif, tampalan hendaklah diuji dan diluluskan terlebih dahulu. 3. Sekiranya tampalan belum sesuai dilaksanakan, gunakan kawalan pampasan (*compensating control*) seperti mengehadkan akses dan meningkatkan pemantauan.
Penyelaras	Pasukan keselamatan ICT / pemilik sistem / pembekal
Bukti pelaksanaan yang disarankan	Daftar kerentanan, tahap risiko, pemilik tindakan, mitigasi sementara dan tarikh sasaran pembetulan.

5. Sahkan Sandaran dan Kebolehpulihan Data

Komponen	Perincian
Tujuan	Memastikan sandaran data kritikal tersedia, selamat dan boleh dipulihkan, termasuk sandaran luar talian atau *immutable backup* bagi membolehkan perkhidmatan dipulihkan sekiranya data rosak, hilang atau disulitkan oleh *ransomware*.
Langkah pelaksanaan	1. Pastikan data, pangkalan data, konfigurasi dan imej sistem yang diperlukan untuk memulihkan perkhidmatan kritikal telah disandarkan. 2. Pastikan sekurang-kurangnya satu salinan diasingkan dan dilindungi daripada pengubahan atau penghapusan, contohnya sandaran luar talian (*offline*) atau *immutable*. 3. Jalankan ujian pemulihan terkawal ke atas sistem kritikal terpilih tanpa menjejaskan operasi. Sahkan data boleh digunakan, fungsi utama sistem beroperasi dan salinan yang dipulihkan tidak memperkenalkan semula ancaman.
Penyelaras	Pasukan keselamatan ICT / pemilik sistem
Bukti pelaksanaan yang disarankan	Tarikh sandaran terakhir, bukti semakan sandaran, keputusan ujian pemulihan dan isu yang perlu diperbaiki.

6. Laksanakan Penilaian Kerentanan dan Ujian Penembusan (*Vulnerability Assessment and Penetration Testing*, VAPT) Secara Bersasar

Komponen	Perincian
Tujuan	VAPT terdiri daripada pemeriksaan kelemahan keselamatan (*Vulnerability Assessment*, VA) dan ujian terkawal untuk menentukan sama ada kelemahan tersebut boleh dieksploitasi (*Penetration Testing*, PT). Tujuannya ialah mengenal pasti risiko sebelum disalahgunakan.
Langkah pelaksanaan	1. Tentukan skop mengikut sistem kritikal dan sistem yang menyimpan maklumat penting.

Komponen	Perincian
	2. Sediakan skop bertulis yang merangkumi sistem yang diuji, jadual dan waktu ujian, pegawai penghubung, kaedah ujian, peraturan pengujian (*rules of engagement*), kaedah pemulihan dan pelan berkaitan. 3. Laksanakan PT secara terkawal oleh personel berkelayakan dengan kelulusan pemilik sistem. 4. Dapatkan laporan kelemahan, tahap risiko, kesan kepada perkhidmatan, cadangan pembetulan, pegawai bertanggungjawab dan tarikh sasaran. 5. Laksanakan pembetulan, jalankan ujian semula (*retest*) bagi mengesahkan kelemahan telah ditangani.
Penyelaras	ICTSO / pemilik sistem / pasukan VAPT yang diberi kuasa/dilantik.
Bukti pelaksanaan yang disarankan	Skop dan kelulusan VAPT, pelan ujian, laporan penemuan berkeutamaan risiko, pelan pembetulan, bukti ujian semula dan penerimaan risiko baki oleh pihak berkuasa yang berkaitan.

7. Perkukuh Kawalan Pembekal dan Hubungan dengan Pihak Ketiga

Komponen	Perincian
Tujuan	Serangan terhadap pembekal boleh turut menjejaskan sistem agensi.
Langkah pelaksanaan	1. Kenal pasti pembekal yang mempunyai akses jauh, menyelenggara sistem penting atau menyimpan data organisasi. Tentukan keutamaan semakan berdasarkan tahap akses, sensitiviti data dan impak gangguan kepada operasi. 2. Semak sambungan pembekal, akses jauh, akaun pentadbiran dan perkhidmatan, akses penyelenggaraan, integrasi API dan pergantungan kepada perkhidmatan awan.

Komponen	Perincian
	3. Minta pembekal kritikal mengesahkan pegawai kecemasan utama dan pengganti, saluran komunikasi alternatif, tempoh pemberitahuan awal, tanggungjawab perkongsian maklumat, kawalan akses dan tatacara pemberitahuan insiden. 4. Sediakan langkah kesinambungan jika pembekal terjejas dengan mengenal pasti kaedah operasi alternatif, sokongan pemulihan dan pilihan peralihan perkhidmatan. 5. Hadkan atau gantung akses yang tidak diperlukan mengikut kelulusan dan keperluan operasi.
Penyelaras	Pasukan ICT / pengurus kontrak / pemilik sistem
Bukti pelaksanaan yang disarankan	Senarai pembekal kritikal dan pihak ketiga berisiko bersama maklumat – sistem atau data terlibat dan tahap akses, status semakan serta pelan mitigasi.

8. Kemas Kini/ Laksanakan Penilaian Risiko, Pelan Respons Insiden dan Pelan Kesinambungan

Komponen	Perincian
Tujuan	Memastikan organisasi masih mampu menyampaikan perkhidmatan penting sekiranya berlaku serangan.
Langkah pelaksanaan	1. Laksanakan penilaian risiko bersasar bagi senario utama seperti *ransomware*, kebocoran data, serangan DDoS, kompromi identiti, pencerobohan laman web dan kegagalan pembekal. 2. Tentukan perkhidmatan yang perlu dipulihkan terlebih dahulu, pegawai pembuat keputusan dan cara perkhidmatan sementara diteruskan. 3. Semak Pelan Respons Insiden (IRP), Pelan Kesinambungan Perkhidmatan (PKP), Pelan Pemulihan Bencana (DRP), sasaran RTO/RPO dan pelan komunikasi krisis.

Komponen	Perincian
	4. Jalankan ujian seperti latihan meja (*tabletop*) ringkas bagi menentukan siapa yang dihubungi, siapa yang meluluskan tindakan dan bagaimana pelanggan dimaklumkan.
Penyelaras	Pihak pengurusan / ICTSO / pemilik perkhidmatan
Bukti pelaksanaan yang disarankan	Daftar risiko yang dikemas kini, keutamaan pemulihan, keputusan latihan meja dan pelan penambahbaikan.

9. Laksanakan Keselamatan Data dan Rangkaian Berkriptografi Penuh

Komponen	Perincian
Tujuan	Memastikan data yang disimpan, diproses dan dihantar sentiasa dilindungi oleh kriptografi yang kukuh, supaya data yang dipintas, dicuri atau diubah tidak boleh dibaca atau disalahgunakan oleh pihak yang tidak dibenarkan.
Langkah pelaksanaan	1. Naik taraf TLS dengan keupayaan terkini dan optimum serta perkukuh penyulitan data dalam simpanan (i) Gunakan TLS 1.3 sebagai keutamaan dan TLS 1.2 sebagai tahap minimum bagi semua portal, aplikasi, API, e-mel, perkakasan dan sambungan antara sistem. Nyahaktif SSL, TLS 1.0 dan TLS 1.1. (ii) Hadkan suite sifer (*cipher suite*) dengan mengutamakan algoritma dalam kategori AKSA MySEAL 2.1 *Approved*, Senarai Algoritma Kriptografi Terpercaya Negara (MySEAL). Algoritma kategori Neutral (contohnya SHA-256) boleh digunakan secara bersyarat dalam tempoh peralihan mengikut syarat yang ditetapkan, manakala algoritma kategori *Monitored* hanya bagi keserasian dengan sistem legasi. Khususnya, nyahaktifkan sifer lemah seperti RC4, 3DES, NULL, EXPORT dan sifer berasaskan MD5 atau SHA-1.

Komponen	Perincian
	(iii) Aktifkan HTTP *Strict Transport Security* (HSTS) dan ubah hala semua trafik HTTP kepada HTTPS. Pastikan penyulitan turut diguna pakai bagi trafik dalaman, bukan hanya trafik yang terdedah ke Internet. (iv) Lindungi data dalam simpanan (*data at rest*) bagi pangkalan data, storan awan dan sandaran menggunakan penyulitan kukuh seperti AES-256, dengan kunci diurus secara berasingan, sebaik-baiknya dalam *Hardware Security Module* (HSM). 2. Kawal sambungan IoT dan OT ke awan melalui pengezonan dan saluran yang selamat (i) Sistem OT dan ICS tidak boleh disambungkan terus ke Internet atau awan. Semua sambungan hendaklah melalui *firewall*, DMZ industri (IDMZ) atau get laluan (*gateway*) yang dikawal, selaras dengan prinsip pengezonan dan saluran (*zones and conduits*) IEC 62443. Peranti IoT yang direka untuk bersambung terus ke awan hendaklah dilindungi dengan kawalan setara. (ii) Sulitkan sambungan IoT/OT ke awan menggunakan TLS dengan pengesahan bersama (*mutual* TLS) atau VPN IPsec, dan gunakan sijil digital unik bagi setiap peranti, bukan kata laluan atau kunci yang dikongsi. (iii) Tukar kelayakan lalai (*default credentials*), nyahaktif perkhidmatan yang tidak diperlukan dan pertimbangkan get laluan satu hala (data *diode*) bagi sistem OT yang paling kritikal. 3. Gunakan PKI dan sijil digital yang sah sahaja (i) Gunakan sijil digital yang dikeluarkan oleh Pihak Berkuasa Pemerakuan (CA) berlesen di bawah Akta Tandatangan Digital 1997 [*Akta 562*], CA awam yang dipercayai atau PKI dalaman organisasi

Komponen	Perincian
	yang diurus dan diaudit. Sijil swa-tandatangan (*self-signed*) tidak wajar digunakan bagi sistem produksi yang terdedah kepada pengguna atau pihak luar. (ii) Sediakan inventori sijil yang merangkumi pemilik, sistem, tarikh luput, algoritma, panjang kunci dan CA pengeluar. Gantikan sijil yang telah luput, hampir luput, dibatalkan atau menggunakan algoritma lemah (contohnya SHA-1 atau RSA kurang daripada 2048 bit). (iii) Laksanakan amalan pengurusan sijil digital terbaik mengikut ketetapan piawaian antarabangsa.
Penyelaras	ICTSO / pentadbir rangkaian dan sistem / pemilik sistem OT / pengurus PKI / pembekal
Bukti pelaksanaan yang disarankan	Rekod konfigurasi TLS dan *suite* sifer yang diguna pakai, senarai sambungan IoT/OT ke awan dan laluan *firewall*/ DMZ yang diluluskan, inventori sijil digital dengan tarikh luput, rekod penggantian sijil serta rekod pengurusan kunci.

10. Gunakan *Application Programming Interface* (*API*) Bertandatangan Digital

Komponen	Perincian
Tujuan	Memastikan setiap permintaan dan respons API adalah tulen, tidak diubah semasa penghantaran dan boleh dikesan kepada penghantarnya, terutamanya bagi API yang mengendalikan transaksi, data peribadi, pembayaran dan integrasi antara agensi atau pembekal.
Langkah pelaksanaan	1. Sediakan senarai semua API yang digunakan, termasuk API dalaman, API awam, API pembekal dan API antara agensi, serta kenal pasti API yang mengendalikan data sensitif atau transaksi kritikal. 2. Laksanakan pengesahan bersama (*mutual* TLS) bagi API antara sistem dan antara organisasi, supaya kedua-dua pihak mengesahkan identiti masing-masing menggunakan sijil digital yang sah.

Komponen	Perincian
	3. Tandatangani muatan (*payload*) atau token akses API secara digital (contohnya JWS/JWT) menggunakan algoritma tandatangan dalam AKSA MySEAL 2.1 *Approved* seperti ECDSA atau RSA-PSS. Sahkan tandatangan pada setiap permintaan, tolak token tanpa tandatangan atau yang menggunakan algoritma tidak dibenarkan, dan urus kunci tandatangan dalam HSM dengan putaran kunci berkala. 4. Log dan pantau kegagalan pengesahan tandatangan, token tidak sah dan corak panggilan API luar biasa melalui SOC/SIEM.
Penyelaras	ICTSO / pemilik aplikasi / pasukan pembangunan / pengurus integrasi / pembekal
Bukti pelaksanaan yang disarankan	Inventori API dan klasifikasi risiko, status pelaksanaan mTLS dan tandatangan digital bagi setiap API kritikal, polisi pengurusan dan putaran kunci, serta log pemantauan kegagalan pengesahan.

11. Laksanakan Inventori dan Audit Penggunaan Kriptografi

Komponen	Perincian
Tujuan	Mengetahui di mana dan bagaimana kriptografi digunakan dalam organisasi, mengenal pasti penggunaan mekanisme kriptografi yang lemah atau terdedah serta menyediakan asas bagi pelaksanaan tindakan pembetulan dan migrasi kriptografi pasca-kuantum (PQC) secara terancang.
Langkah pelaksanaan	1. Bangunkan dan kemas kini inventori kriptografi (*Cryptographic Bill of Materials* – CBOM) yang merangkumi aset ICT, algoritma, panjang kunci, protokol, pustaka kriptografi, sijil digital, HSM, lokasi penggunaan, pemilik sistem dan klasifikasi maklumat yang dilindungi. 2. Laksanakan audit penggunaan kriptografi bagi mengenal pasti algoritma dan protokol yang lemah, lapuk atau tidak lagi disyorkan. Utamakan penggunaan algoritma kriptografi yang disenaraikan dalam Senarai

Komponen	Perincian
	Algoritma Kriptografi Terpercaya Negara (MySEAL), mengikut kategori, fungsi penggunaan dan keperluan keselamatan. 3. Audit amalan pengurusan kunci kriptografi merangkumi penjanaan, penyimpanan, pengedaran, putaran, sandaran, pembatalan dan pemusnahan kunci, termasuk pengasingan tugas serta kawalan akses kepada HSM. 4. Nilai tahap ketangkasan kriptografi (*crypto-agility*) dan kebergantungan terhadap sistem legasi, vendor serta komponen teknologi bagi memastikan organisasi berupaya melaksanakan perubahan algoritma atau protokol secara terkawal. 5. Rancang migrasi PQC secara berperingkat dengan mengambil kira algoritma yang disenaraikan dalam AKSA MySEAL 2.1 *Approved*, termasuk ML-KEM (FIPS 203), ML-DSA (FIPS 204) dan SLH-DSA (FIPS 205), berdasarkan kesesuaian fungsi, sistem kritikal dan penilaian risiko. Pertimbangkan keperluan sokongan PQC dalam perolehan baharu serta kontrak pembekal. 6. Masukkan dapatan inventori dan audit kriptografi ke dalam daftar risiko serta pelan tindakan pembetulan.
Penyelaras	Pihak pengurusan / ICTSO / CISO / pemilik sistem / juruaudit dalaman / pembekal
Bukti pelaksanaan yang disarankan	Inventori kriptografi (termasuk CBOM), laporan audit penggunaan dan pengurusan kunci kriptografi, daftar risiko, pelan tindakan pembetulan serta pelan migrasi PQC.

12. Lapor, Eskalasi dan Pantau Penutupan Tindakan

Komponen	Perincian
Tujuan	Memastikan insiden dikendalikan dengan segera dan pihak berkuasa (NACSA) menerima pemberitahuan mengikut peraturan yang terpakai.
Langkah pelaksanaan	1. Sekiranya insiden disyaki, aktifkan prosedur respons serta-merta. Eskalasi dan pelaporan tidak perlu menunggu laporan VAPT atau siasatan teknikal yang lengkap. 2. Patuhi saluran, tempoh dan kaedah pelaporan yang diwajibkan. 3. Bentangkan status ringkas kepada pengurusan, merangkumi tindakan yang telah dan belum selesai, insiden, risiko baki, pemilik tindakan, tarikh sasaran dan kesediaan pemulihan.
Penyelaras	ICTSO / pasukan respons insiden / pengurusan
Bukti pelaksanaan yang disarankan	Rekod insiden dan pelaporan, bukti pemberitahuan (jika berkaitan), status tindakan dan keputusan pengurusan.

C. PENYELARASAN STATUS LAPORAN DALAMAN KESIAPSIAGAAN

Bagi tujuan pemantauan dan penyelarasan tahap kesiapsiagaan keselamatan siber di peringkat organisasi masing-masing, setiap organisasi disarankan untuk menggunakan Templat Senarai Semak Status Tindakan Kesiapsiagaan C1 sebagai panduan penyediaan laporan status awal kesiapsiagaan.

Laporan status tindakan kesiapsiagaan ini adalah untuk tujuan pemantauan dan pelaporan dalaman organisasi sahaja serta tidak perlu dikemukakan kepada Agensi Keselamatan Siber Negara (NACSA), kecuali apabila diminta secara rasmi oleh NACSA.

Sekiranya terdapat petunjuk kompromi atau insiden keselamatan siber, tindakan pengasingan, pemeliharaan bukti, eskalasi dan pemberitahuan hendaklah dilaksanakan dengan segera mengikut prosedur yang terpakai.

C1: Templat Senarai Semak Status Tindakan Kesiapsiagaan

Keutamaan dan Tindakan	Maklumat Minimum	Status	Catatan
1.Aktifkan Penyelarasan, Tetapkan Pegawai Bertanggungjawab dan Saluran Komunikasi	Senarai sistem kritikal dan nama dan nombor pegawai bertanggungjawab untuk dihubungi	Belum mula / Dalam tindakan / Selesai	
2.Kenal Pasti Tanda Kompromi dan Ancaman Aktif	Maklumat Amaran kritikal SOC/SIEM/EDR dan tindakan triage	Belum mula / Dalam tindakan / Selesai	
3.Lindungi Akses dan Permukaan Serangan Siber (*Attack Surface*)	Maklumat MFA, akaun istimewa, akses VPN dan vendor	Belum mula / Dalam tindakan / Selesai	
4.Semak Kerentanan dan Laksanakan Tampalan (*Patch*) Kritikal	Maklumat berhubung Isu berkaitan, mitigasi sementara, tarikh penutupan	Belum mula / Dalam tindakan / Selesai	
5.Sahkan Sandaran dan Kebolehpulihan Data	Status sandaran dan keputusan ujian pemulihan	Belum mula / Dalam tindakan / Selesai	
6.Laksanakan Penilaian Kerentanan dan Ujian Penembusan (VAPT) Secara Bersasar	Skop, kelulusan, penemuan kritikal, status ujian semula	Belum mula / Dalam tindakan / Selesai	
7. Perkukuh Kawalan Pembekal dan Hubungan Dengan Pihak Ketiga	Maklumat pembekal kritikal disemak dan isu tertunggak	Belum mula / Dalam tindakan / Selesai	
8.Kemas Kini/ Laksanakan Penilaian Risiko, Pelan Respons Insiden dan Pelan Kesinambungan	IRP/PKP/DRP, latihan meja dan risiko baki	Belum mula / Dalam tindakan / Selesai	

Keutamaan dan Tindakan	Maklumat Minimum	Status	Catatan
9.Laksanakan Keselamatan Data dan Rangkaian Berkriptografi Penuh	Konfigurasi TLS, sambungan IoT/OT melalui firewall/DMZ, status sijil digital	Belum mula / Dalam tindakan / Selesai	
10.Gunakan API Bertandatangan Digital	API kritikal dengan mTLS dan tandatangan digital, pengurusan kunci	Belum mula / Dalam tindakan / Selesai	
11.Laksanakan Inventori dan Audit Penggunaan Kriptografi	Status CBOM, kriptografi lemah/terdedah kuantum, pelan migrasi PQC	Belum mula / Dalam tindakan / Selesai	
12.Lapor, Eskalasi dan Pantau Penutupan Tindakan	Bilangan insiden, impak, eskalasi dan pelaporan	Belum mula / Dalam tindakan / Selesai	

D. RUJUKAN PERUNDANGAN DAN PENTADBIRAN

(i) Akta Keselamatan Siber 2024 [*Akta 854*].
(ii) Peraturan-Peraturan Keselamatan Siber (Tempoh bagi Penilaian Risiko Keselamatan Siber dan Audit) 2024 [P.U.(A) 219/2024].
(iii) Peraturan-Peraturan Keselamatan Siber (Pemberitahuan Insiden Keselamatan Siber) 2024 [P.U.(A) 220/2024].
(iv) Arahan Ketua Eksekutif NACSA No. 1 – Pemberitahuan Insiden Keselamatan Siber.
(v) Arahan Ketua Eksekutif NACSA No. 4 – Penilaian Kendiri Garis Asas Keselamatan Siber (*National Cyber Security Baseline Self Assessment*).
(vi) Arahan Ketua Eksekutif NACSA No. 5 – Penilaian Risiko Keselamatan Siber.
(vii) Arahan Ketua Eksekutif NACSA No. 7 – Penyediaan Tataamalan oleh Ketua Sektor Infrastruktur Maklumat Kritikal Negara dan Pemakaiannya.
(viii) Arahan Ketua Eksekutif NACSA No. 8 – Audit Berhubung Keselamatan Siber bagi Entiti Infrastruktur Maklumat Kritikal Negara.
(ix) Arahan Ketua Eksekutif NACSA No. 9 – Penyediaan Data dan Maklumat Pelaksanaan Migrasi Kriptografi Pasca Kuantum oleh Entiti Infrastruktur Maklumat Kritikal Negara.
(x) Arahan Ketua Eksekutif NACSA No. 10 – Pemakaian Pelan Pengurusan Krisis Keselamatan Siber Negara.
(xi) Pekeliling Am Bil. 4 Tahun 2022 – Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam.
(xii) Surat Pekeliling Am Bil. 3 Tahun 2024 – Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam.
(xiii) Surat Pekeliling Am Bil. 4 Tahun 2024 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam
(xiv) Polisi keselamatan siber, DRP/PKP dan garis panduan yang berkaitan.
(xv) Arahan dan pekeliling di atas tertakluk pada pemakaian dan versi yang berkuat kuasa.

E. MAKLUMAT PERHUBUNGAN

Bagi sebarang pertanyaan lanjut berhubung dengan Garis Panduan ini, boleh dikemukan melalui e-mel **auditpematuhan@nacsa.gov.my**.

F. PENUTUP

Kerjasama dan perhatian serius semua pihak dalam melaksanakan langkah kesiapsiagaan ini amatlah dihargai. Pelaksanaan secara terancang, berasaskan risiko dan di bawah pengawasan pengurusan adalah penting bagi memastikan keselamatan dan kesinambungan penyampaian perkhidmatan negara sentiasa terpelihara.