

D.R. 8/2023

RANG UNDANG-UNDANG KESELAMATAN SIBER 2024

PINDAAN DALAM JAWATANKUASA

TEKS BAHASA KEBANGSAAN

Fasal 58

Subperenggan 58(b)(i) Rang Undang-Undang dipinda dengan menggantikan perkataan “dan” di hujung subperenggan itu dengan perkataan “atau”.

—————

HURAIAN

Fasal 58 Rang Undang-Undang dipinda dalam subperenggan 58(b)(i) untuk menjelaskan lagi peruntukan yang berhubungan dengan fakta yang perlu dibuktikan oleh seorang pengarah, pegawai pematuhan, pekongsi, pengurus, setiausaha atau pegawai lain yang seumpamanya bagi suatu syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain dalam hal keadaan apabila syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain didapati bersalah atas suatu kesalahan di bawah Rang Undang-Undang ini.

D.R. 8/2024

RANG UNDANG-UNDANG KESELAMATAN SIBER 2024

SUSUNAN FASAL

BAHAGIAN I

PERMULAAN

Fasal

1. Tajuk ringkas dan permulaan kuat kuasa
2. Akta ini mengikat Kerajaan Persekutuan dan Kerajaan Negeri
3. Pemakaian luar wilayah
4. Tafsiran

BAHAGIAN II

JAWATANKUASA KESELAMATAN SIBER NEGARA

5. Penubuhan Jawatankuasa
6. Fungsi Jawatankuasa
7. Mesyuarat Jawatankuasa
8. Jawatankuasa boleh mengundang orang lain untuk menghadiri mesyuarat
9. Jawatankuasa boleh menubuhkan jawatankuasa kecil

BAHAGIAN III

KEWAJIPAN DAN KUASA KETUA EKSEKUTIF

10. Kewajipan dan kuasa Ketua Eksekutif
11. Sistem Pusat Penyelarasan dan Kawalan Siber Negara
12. Pelantikan pakar keselamatan siber
13. Arahan Ketua Eksekutif
14. Kuasa untuk mengumpul maklumat

Rang Undang-Undang

BAHAGIAN IV

KETUA SEKTOR INFRASTRUKTUR MAKLUMAT KRITIKAL NEGARA DAN ENTITI INFRASTRUKTUR MAKLUMAT KRITIKAL NEGARA

Fasal

15. Pelantikan ketua sektor infrastruktur maklumat kritikal negara
16. Fungsi ketua sektor infrastruktur maklumat kritikal negara
17. Penetapan entiti infrastruktur maklumat kritikal negara
18. Penetapan ketua sektor infrastruktur maklumat kritikal negara sebagai entiti infrastruktur maklumat kritikal negara
19. Pembatalan penetapan entiti infrastruktur maklumat kritikal negara
20. Kewajipan untuk memberikan maklumat yang berhubungan dengan infrastruktur maklumat kritikal negara
21. Kewajipan untuk melaksanakan tataamalan
22. Kewajipan untuk membuat penilaian risiko keselamatan siber dan audit
23. Kewajipan untuk memberikan pemberitahuan mengenai insiden keselamatan siber
24. Latihan keselamatan siber

BAHAGIAN V

TATAAMALAN

25. Tataamalan
26. Arahan di bawah undang-undang bertulis yang lain hendaklah selaras dengan tataamalan

BAHAGIAN VI

PEMBERI PERKHIDMATAN KESELAMATAN SIBER

27. Pelesenan pemberi perkhidmatan keselamatan siber
28. Kelayakan bagi permohonan lesen
29. Permohonan bagi lesen
30. Pembaharuan lesen
31. Syarat lesen
32. Kewajipan untuk menyimpan dan menyenggara rekod
33. Pembatalan atau penggantungan lesen
34. Pemindahmilikan atau penyerahhakan lesen

BAHAGIAN VII

INSIDEN KESELAMATAN SIBER

Fasal

35. Insiden keselamatan siber

BAHAGIAN VIII

PENGUATKUASAAN

36. Pemberikuasaan pegawai awam
37. Kad kuasa
38. Kuasa penyiasatan
39. Penggeledahan dan penyitaan dengan waran
40. Penggeledahan dan penyitaan tanpa waran
41. Senarai objek, dsb., yang disita
42. Kos memegang objek, dsb., yang disita
43. Pelepasan objek, dsb., yang disita
44. Pelucuthakan objek, dsb., yang disita
45. Hak harta mengenai objek, dsb., yang dilucuthakkan
46. Akses kepada data berkomputer
47. Tiada kos atau ganti rugi yang berbangkit daripada penyitaan boleh didapatkan
48. Kuasa untuk menghendaki kehadiran orang yang mempunyai pengetahuan tentang kes
49. Pemeriksaan orang yang mempunyai pengetahuan tentang kes
50. Kebolehterimaan pernyataan sebagai keterangan
51. Kuasa tambahan
52. Halangan

BAHAGIAN IX

AM

53. Rayuan
54. Penyampaian dokumen
55. Kewajipan kerahsiaan
56. Perlindungan daripada guaman dan prosiding undang-undang

Fasal

57. Pendakwaan
58. Tanggungan pengarah, dsb., bagi syarikat, dsb.
59. Tanggungan seseorang bagi perbuatan, dsb., pekerja, dsb.
60. Pengkompaunan kesalahan
61. Kuasa untuk mengecualikan
62. Kuasa untuk meminda Jadual
63. Kuasa untuk membuat peraturan-peraturan
64. Kecualian

JADUAL

RANG UNDANG-UNDANG

b e r n a m a

Suatu Akta untuk meningkatkan keselamatan siber negara dengan mengadakan peruntukan bagi penubuhan Jawatankuasa Keselamatan Siber Negara, kewajipan dan kuasa Ketua Eksekutif Agensi Keselamatan Siber Negara, fungsi dan kewajipan ketua sektor infrastruktur maklumat kritikal negara dan entiti infrastruktur maklumat kritikal negara dan pengurusan ancaman keselamatan siber dan insiden keselamatan siber terhadap infrastruktur maklumat kritikal negara, untuk mengawal selia pemberi perkhidmatan keselamatan siber melalui pelesenan, dan untuk mengadakan peruntukan bagi perkara yang berkaitan.

[]

DIPERBUAT oleh Parlimen Malaysia seperti yang berikut:

BAHAGIAN I

PERMULAAN

Tajuk ringkas dan permulaan kuat kuasa

1. (1) Akta ini bolehlah dinamakan Akta Keselamatan Siber 2024.

(2) Akta ini mula berkuat kuasa pada tarikh yang ditetapkan oleh Menteri melalui pemberitahuan dalam *Warta*.

Akta ini mengikat Kerajaan Persekutuan dan Kerajaan Negeri

2. (1) Akta ini hendaklah mengikat Kerajaan Persekutuan dan Kerajaan Negeri.

(2) Tiada apa-apa pun jua dalam Akta ini boleh menyebabkan Kerajaan Persekutuan dan Kerajaan Negeri didakwa bagi mana-mana kesalahan di bawah Akta ini.

Pemakaian luar wilayah

3. (1) Akta ini hendaklah, berhubung dengan mana-mana orang, walau apa pun kerakyatan atau kewarganegaraannya, mempunyai kuat kuasa di luar dan juga di dalam Malaysia, dan jika suatu kesalahan di bawah Akta ini dilakukan oleh mana-mana orang di mana-mana tempat di luar Malaysia, dia boleh diuruskan berkenaan dengan kesalahan itu seolah-olah kesalahan itu telah dilakukan di mana-mana tempat di dalam Malaysia.

(2) Bagi maksud subseksyen (1), Akta ini hendaklah terpakai jika bagi kesalahan yang berkenaan, infrastruktur maklumat kritikal negara itu berada secara keseluruhannya atau sebahagiannya di dalam Malaysia.

Tafsiran

4. Dalam Akta ini, melainkan jika konteksnya menghendaki makna yang lain—

“Akta ini” termasuklah mana-mana perundangan subsidiari yang dibuat di bawah Akta ini;

“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;

“arahan” ertinya suatu arahan yang dikeluarkan oleh Ketua Eksekutif di bawah seksyen 13;

“ditetapkan” ertinya ditetapkan oleh Menteri melalui peraturan-peraturan yang dibuat di bawah Akta ini;

“entiti infrastruktur maklumat kritikal negara” ertinya mana-mana Entiti Kerajaan atau orang yang ditetapkan sebagai entiti infrastruktur maklumat kritikal negara di bawah seksyen 17 atau 18;

“Entiti Kerajaan” ertinya—

- (a) mana-mana kementerian, jabatan, pejabat, agensi, pihak berkuasa, suruhanjaya, jawatankuasa, lembaga, majlis atau badan lain, bagi Kerajaan Persekutuan, atau bagi mana-mana Kerajaan Negeri, yang ditubuhkan di bawah mana-mana undang-undang bertulis atau selainnya; dan
- (b) mana-mana pihak berkuasa tempatan;

“infrastruktur maklumat kritikal negara” ertinya suatu komputer atau sistem komputer yang gangguan pada atau kemusnahan komputer atau sistem komputer itu boleh membawa kesan yang memudaratkan terhadap penyampaian apa-apa perkhidmatan yang perlu bagi keselamatan, pertahanan, hubungan luar negara, ekonomi, kesihatan awam, kesejahteraan awam atau ketenteraman awam di Malaysia, atau terhadap keupayaan Kerajaan Persekutuan atau mana-mana Kerajaan Negeri untuk menjalankan fungsinya secara berkesan;

“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;

“Jawatankuasa” ertinya Jawatankuasa Keselamatan Siber Negara yang ditubuhkan di bawah seksyen 5;

“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;

“Ketua Eksekutif” ertinya Ketua Eksekutif Agensi Keselamatan Siber Negara;

“ketua sektor infrastruktur maklumat kritikal negara” ertinya mana-mana Entiti Kerajaan atau orang yang dilantik sebagai ketua sektor infrastruktur maklumat kritikal negara di bawah seksyen 15;

“komputer” ertinya suatu peranti elektronik, magnet, optik, elektrokimia, atau peranti pemprosesan data yang lain yang melaksanakan fungsi logik, aritmetik, storan atau paparan, dan termasuklah apa-apa kemudahan storan data atau kemudahan komunikasi yang berkaitan secara langsung dengan atau dikendali bersama dengan suatu peranti, tetapi tidak termasuk suatu mesin taip atau mesin pengatur huruf berautomat, atau suatu mesin kira pegang tangan mudah alih atau peranti seumpama yang lain yang tidak boleh diprogram atau yang tidak mengandungi apa-apa kemudahan storan data;

“Menteri” ertinya Menteri yang dipertanggungjawabkan dengan tanggungjawab bagi keselamatan siber;

“pegawai diberi kuasa” ertinya mana-mana pegawai polis yang apa jua pun pangkatnya atau mana-mana pegawai awam yang diberi kuasa di bawah seksyen 36;

“pemberi perkhidmatan keselamatan siber” ertinya seseorang yang memberikan perkhidmatan keselamatan siber;

“perkhidmatan keselamatan siber” ertinya perkhidmatan keselamatan siber sebagaimana yang ditetapkan di bawah subseksyen 27(2);

“sektor infrastruktur maklumat kritikal negara” ertinya sektor infrastruktur maklumat kritikal negara yang dinyatakan dalam Jadual;

“sistem komputer” ertinya suatu pengaturan komputer yang saling bersambung yang direka bentuk untuk melaksanakan satu atau lebih fungsi spesifik, dan termasuklah—

- (a) sistem teknologi maklumat; dan
- (b) sistem teknologi pengendalian seperti sistem kawalan industri, pengawal logik boleh atur cara, sistem kawalan penyeliaan dan pemerolehan data, atau sistem kawalan teragih;

“tataamalan” ertinya tataamalan yang disebut di bawah seksyen 25.

BAHAGIAN II

JAWATANKUASA KESELAMATAN SIBER NEGARA

Penubuhan Jawatankuasa

5. (1) Suatu jawatankuasa dengan nama “Jawatankuasa Keselamatan Siber Negara” ditubuhkan.

(2) Jawatankuasa hendaklah terdiri daripada anggota yang berikut:

- (a) Perdana Menteri yang hendaklah menjadi Pengerusi;
- (b) Menteri yang dipertanggungkan dengan tanggungjawab bagi kewangan;
- (c) Menteri yang dipertanggungkan dengan tanggungjawab bagi hal ehwal luar negeri;
- (d) Menteri yang dipertanggungkan dengan tanggungjawab bagi pertahanan;
- (e) Menteri yang dipertanggungkan dengan tanggungjawab bagi hal ehwal dalam negeri;
- (f) Menteri yang dipertanggungkan dengan tanggungjawab bagi komunikasi;

- (g) Menteri yang dipertanggungjawabkan dengan tanggungjawab bagi perkara berkaitan digital;
 - (h) Ketua Setiausaha Negara;
 - (i) Panglima Angkatan Tentera;
 - (j) Ketua Polis Negara;
 - (k) Ketua Pengarah Keselamatan Negara; dan
 - (l) tidak lebih daripada dua orang lain yang hendaklah dilantik oleh Jawatankuasa dalam kalangan orang yang mempunyai kedudukan dan pengalaman dalam keselamatan siber.
- (3) Pengerusi hendaklah melantik dalam kalangan anggota Jawatankuasa seorang Timbalan Pengerusi.
- (4) Ketua Eksekutif hendaklah menjadi setiausaha kepada Jawatankuasa.

Fungsi Jawatankuasa

6. (1) Jawatankuasa hendaklah mempunyai fungsi yang berikut:
- (a) untuk merancang, merumus dan memutuskan dasar yang berhubungan dengan keselamatan siber negara;
 - (b) untuk memutuskan mengenai pendekatan dan strategi dalam menangani perkara yang berhubungan dengan keselamatan siber negara;
 - (c) untuk mengawasi pelaksanaan dasar dan strategi yang berhubungan dengan keselamatan siber negara;
 - (d) untuk menasihati dan membuat syor kepada Kerajaan Persekutuan mengenai polisi dan langkah strategik untuk mengukuhkan keselamatan siber negara;
 - (e) untuk memberikan arahan kepada Ketua Eksekutif dan ketua sektor infrastruktur maklumat kritikal negara mengenai perkara yang berhubungan dengan keselamatan siber negara;

- (f) untuk menyelia pelaksanaan yang berkesan Akta ini; dan
- (g) untuk melakukan apa-apa perkara lain yang timbul atau berbangkit daripada fungsi Jawatankuasa di bawah Akta ini selaras dengan maksud Akta ini.

(2) Jawatankuasa hendaklah mempunyai segala kuasa sebagaimana yang perlu bagi, atau berkaitan dengan, atau yang semunasabahnya bersampungan dengan, pelaksanaan fungsinya di bawah Akta ini.

Mesyuarat Jawatankuasa

7. (1) Jawatankuasa hendaklah mengadakan mesyuaratnya seberapa kerap sebagaimana yang ditentukan oleh Pengerusi dan mesyuarat hendaklah diadakan pada masa dan di tempat sebagaimana yang ditentukan oleh Pengerusi.

(2) Pengerusi hendaklah mempengerusikan semua mesyuarat Jawatankuasa.

(3) Jika Pengerusi tidak hadir pada mana-mana mesyuarat Jawatankuasa, dia boleh mengarahkan Timbalan Pengerusi untuk menggantikannya sebagai pengerusi mesyuarat itu.

(4) Kuorum Jawatankuasa ialah lima.

(5) Pengerusi boleh membenarkan penggunaan suatu rangkaian video secara langsung, rangkaian televisyen secara langsung atau apa-apa cara komunikasi elektronik yang lain bagi maksud apa-apa mesyuarat Jawatankuasa.

(6) Jawatankuasa boleh menentukan tataranya sendiri.

Jawatankuasa boleh mengundang orang lain untuk menghadiri mesyuarat

8. Jawatankuasa boleh mengundang mana-mana orang untuk menghadiri mesyuarat Jawatankuasa bagi menasihati Jawatankuasa mengenai apa-apa perkara yang sedang dibincangkan.

Jawatankuasa boleh menubuhkan jawatankuasa kecil

9. (1) Jawatankuasa boleh menubuhkan apa-apa jawatankuasa kecil sebagaimana yang difikirkannya perlu atau suai manfaat untuk membantu Jawatankuasa dalam pelaksanaan fungsinya.

(2) Jawatankuasa boleh melantik mana-mana orang untuk menjadi anggota mana-mana jawatankuasa kecil yang ditubuhkan di bawah subseksyen (1).

(3) Jawatankuasa boleh melantik mana-mana anggotanya atau mana-mana orang lain untuk menjadi pengerusi jawatankuasa kecil yang ditubuhkan di bawah subseksyen (1).

(4) Jawatankuasa kecil hendaklah tertakluk kepada dan bertindak mengikut apa-apa arahan yang diberikan oleh Jawatankuasa.

(5) Jawatankuasa kecil hendaklah bermesyuarat seberapa kerap yang perlu pada masa dan di tempat sebagaimana yang ditentukan oleh pengerusi jawatankuasa kecil itu.

(6) Jawatankuasa kecil boleh mengundang mana-mana orang untuk menghadiri mesyuarat jawatankuasa kecil bagi menasihati jawatankuasa kecil mengenai apa-apa perkara yang sedang dibincangkan.

(7) Pengerusi jawatankuasa kecil boleh membenarkan penggunaan suatu rangkaian video secara langsung, rangkaian televisyen secara langsung atau apa-apa cara komunikasi elektronik yang lain bagi maksud apa-apa mesyuarat jawatankuasa kecil.

BAHAGIAN III**KEWAJIPAN DAN KUASA KETUA EKSEKUTIF****Kewajipan dan kuasa Ketua Eksekutif**

10. (1) Ketua Eksekutif hendaklah mempunyai kewajipan yang berikut:

- (a) untuk menasihati dan membuat syor kepada Jawatankuasa mengenai dasar, strategi dan langkah strategik yang berhubungan dengan keselamatan siber negara;

- (b) untuk melaksanakan dasar, strategi dan langkah strategik yang dibuat dan arahan yang diberikan oleh Jawatankuasa atau Kerajaan Persekutuan mengenai perkara yang berhubungan dengan keselamatan siber negara;
- (c) untuk menyelaras dan mengawasi pelaksanaan dasar, strategi dan langkah strategik mengenai keselamatan siber negara oleh ketua sektor infrastruktur maklumat kritikal negara, entiti infrastruktur maklumat kritikal negara, Entiti Kerajaan atau mana-mana orang lain;
- (d) untuk mengumpul dan menyelaras data, maklumat atau risikan yang berhubungan dengan keselamatan siber negara yang diterima daripada ketua sektor infrastruktur maklumat kritikal negara, entiti infrastruktur maklumat kritikal negara, Entiti Kerajaan atau mana-mana orang lain, dan untuk menilai atau menghubungkan data, maklumat atau risikan itu;
- (e) untuk menyebarkan maklumat dan risikan yang disebut dalam perenggan (d) kepada ketua sektor infrastruktur maklumat kritikal negara atau entiti infrastruktur maklumat kritikal negara jika Ketua Eksekutif fikirkan adalah penting untuk berbuat demikian demi keselamatan siber negara;
- (f) untuk mengeluarkan arahan kepada ketua sektor infrastruktur maklumat kritikal negara, entiti infrastruktur maklumat kritikal negara, Entiti Kerajaan atau mana-mana orang lain mengenai perkara yang berhubungan dengan keselamatan siber negara; atau
- (g) untuk menjalankan apa-apa kewajipan lain yang dikenakan ke atasnya di bawah Akta ini atau sebagaimana yang diarahkan oleh Jawatankuasa.

(2) Ketua Eksekutif hendaklah mempunyai semua kuasa yang perlu bagi, atau berkaitan dengan, atau semunasabahnya bersampingan dengan, penjalanan kewajibannya di bawah Akta ini.

Sistem Pusat Penyelarasan dan Kawalan Siber Negara

11. (1) Ketua Eksekutif hendaklah menubuhkan dan menyenggara suatu sistem keselamatan siber negara yang dikenali sebagai “Sistem Pusat Penyelarasan dan Kawalan Siber Negara” bagi maksud menguruskan ancaman keselamatan siber dan insiden keselamatan siber.

(2) Sistem Pusat Penyelarasan dan Kawalan Siber Negara boleh mengandungi apa-apa data atau maklumat mengenai keselamatan siber yang diperolehi atau disimpan oleh Ketua Eksekutif dalam menjalankan kewajipannya di bawah Akta ini.

(3) Ketua Eksekutif boleh, demi kepentingan keselamatan siber negara dan tertakluk kepada terma dan syarat sebagaimana yang difikirkannya patut, membenarkan mana-mana orang untuk mempunyai akses kepada Sistem Pusat Penyelarasan dan Kawalan Siber Negara.

Pelantikan pakar keselamatan siber

12. Ketua Eksekutif boleh secara bertulis melantik mana-mana pakar yang berkelayakan dalam keselamatan siber sebagai pakar keselamatan siber bagi suatu tempoh sebagaimana yang ditentukan oleh Ketua Eksekutif dalam penjalanan, atau berkaitan dengan, atau semunasabahnya bersampingan dengan, pelaksanaan kewajipan Ketua Eksekutif di bawah Akta ini.

Arahan Ketua Eksekutif

13. (1) Ketua Eksekutif boleh mengeluarkan apa-apa arahan sebagaimana yang didapati perlu oleh Ketua Eksekutif bagi maksud memastikan pematuhan Akta ini.

(2) Ketua Eksekutif boleh membatalkan, mengubah, menyemak semula atau meminda keseluruhan atau mana-mana bahagian apa-apa arahan yang dikeluarkan di bawah seksyen ini.

Kuasa untuk mengumpul maklumat

14. (1) Walau apa pun mana-mana undang-undang bertulis lain, jika Ketua Eksekutif mempunyai alasan yang munasabah untuk mempercayai bahawa mana-mana orang—

(a) mempunyai apa-apa maklumat, butir-butir atau dokumen yang berkaitan dengan pelaksanaan kewajipan dan kuasa Ketua Eksekutif di bawah Akta ini; atau

- (b) berupaya untuk memberikan apa-apa keterangan yang Ketua Eksekutif mempunyai alasan yang munasabah untuk mempercayai adalah berkaitan dengan pelaksanaan kewajipan dan kuasa Ketua Eksekutif di bawah Akta ini,

Ketua Eksekutif boleh, melalui notis secara bertulis, mengarahkan orang itu—

- (A) supaya memberikan apa-apa maklumat atau butir-butir sedemikian kepada Ketua Eksekutif mengikut bentuk dan cara dan dalam tempoh sebagaimana yang dinyatakan dalam notis itu atau apa-apa tempoh lanjutan sebagaimana yang diberikan oleh Ketua Eksekutif;
- (B) supaya mengemukakan apa-apa dokumen sedemikian, sama ada dalam bentuk fizikal atau media elektronik, kepada Ketua Eksekutif mengikut cara dan dalam tempoh sebagaimana yang dinyatakan dalam notis itu atau apa-apa tempoh lanjutan sebagaimana yang diberikan oleh Ketua Eksekutif;
- (C) supaya membuat salinan apa-apa dokumen sedemikian dan mengemukakan salinan itu kepada Ketua Eksekutif mengikut cara dan dalam tempoh sebagaimana yang dinyatakan dalam notis itu atau apa-apa tempoh lanjutan sebagaimana yang diberikan oleh Ketua Eksekutif;
- (D) jika orang itu ialah seorang individu, supaya hadir di hadapan seorang pegawai diberi kuasa pada masa dan di tempat yang dinyatakan dalam notis itu untuk memberikan apa-apa keterangan, sama ada secara lisan atau bertulis, dan mengemukakan apa-apa dokumen, sama ada dalam bentuk fizikal atau media elektronik, mengikut cara dan dalam tempoh sebagaimana yang dinyatakan dalam notis itu atau apa-apa tempoh lanjutan sebagaimana yang diberikan oleh Ketua Eksekutif;
- (E) jika orang itu ialah suatu pertubuhan perbadanan atau badan awam, supaya menyebabkan seorang pegawai berwibawa pertubuhan perbadanan atau badan awam itu untuk hadir di hadapan seorang pegawai diberi kuasa pada masa dan di tempat yang dinyatakan dalam notis itu untuk memberikan apa-apa keterangan, sama ada secara lisan atau bertulis, dan mengemukakan

apa-apa dokumen, sama ada dalam bentuk fizikal atau media elektronik, mengikut cara dan dalam tempoh sebagaimana yang dinyatakan dalam notis itu atau apa-apa tempoh lanjutan sebagaimana yang diberikan oleh Ketua Eksekutif; atau

- (F) jika orang itu ialah suatu perkongsian, supaya menyebabkan seorang individu yang merupakan seorang rakan kongsi dalam perkongsian itu atau seorang pekerja dalam perkongsian itu untuk hadir di hadapan seorang pegawai diberi kuasa pada masa dan di tempat yang dinyatakan dalam notis itu untuk memberikan apa-apa keterangan, sama ada secara lisan atau bertulis, dan mengemukakan apa-apa dokumen, sama ada dalam bentuk fizikal atau media elektronik, mengikut cara dan dalam tempoh sebagaimana yang dinyatakan dalam notis itu atau apa-apa tempoh lanjutan sebagaimana yang diberikan oleh Ketua Eksekutif.

(2) Jika Ketua Eksekutif mengarahkan mana-mana orang untuk mengemukakan apa-apa dokumen di bawah subsekyen (1) dan dokumen itu tiada dalam jagaan orang itu, orang itu hendaklah—

- (a) menyatakan, sepanjang pengetahuan dan kepercayaannya, di mana dokumen itu boleh dijumpai; dan
- (b) mengenal pasti, sepanjang pengetahuan dan kepercayaannya, orang terakhir yang mempunyai jagaan ke atas dokumen itu dan menyatakan, sepanjang pengetahuan dan kepercayaannya, di mana orang terakhir yang disebut itu boleh dijumpai.

(3) Mana-mana orang yang diarahkan untuk memberikan atau mengemukakan apa-apa maklumat, butir-butir atau dokumen atau salinan apa-apa dokumen di bawah subseksyen (1), hendaklah memastikan bahawa maklumat, butir-butir atau dokumen atau salinan dokumen yang diberikan atau dikemukakan itu adalah benar, tepat dan lengkap dan orang itu hendaklah memberikan representasi yang nyata yang bermaksud sedemikian, termasuk suatu perisytiharan bahawa dia tidak menyedari mengenai apa-apa maklumat, butir-butir atau dokumen lain yang akan menjadikan maklumat, butir-butir atau dokumen yang diberikan atau dikemukakan itu tidak benar atau mengelirukan.

(4) Jika mana-mana orang yang menzahirkan apa-apa maklumat atau butir-butir atau mengemukakan apa-apa dokumen sebagai jawapan kepada notis secara bertulis di bawah seksyen ini, orang itu, ejennya atau pekerjanya, atau mana-mana orang lain yang bertindak bagi pihaknya atau di bawah arahnya, tidak boleh, semata-mata oleh sebab penzahiran atau pengemukaan itu, didakwa bagi apa-apa kesalahan di bawah mana-mana undang-undang bertulis, atau dikenakan apa-apa prosiding atau tuntutan oleh mana-mana orang di bawah mana-mana undang-undang atau di bawah apa-apa kontrak, perjanjian atau perkiraan, atau selainnya.

(5) Subseksyen (4) tidaklah menghalang, mencegah atau melarang pemulaan apa-apa pendakwaan bagi apa-apa kesalahan sebagaimana yang diperuntukkan oleh seksyen ini atau penzahiran atau pengemukaan maklumat atau dokumen palsu berhubung dengan suatu notis secara bertulis di bawah seksyen ini yang diberikan kepada Ketua Eksekutif menurut seksyen ini.

(6) Mana-mana orang yang tidak mematuhi arahan Ketua Eksekutif di bawah subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus ribu ringgit atau dipenjara selama tempoh tidak melebihi tiga tahun atau kedua-duanya.

(7) Mana-mana orang yang melanggar subseksyen (2) atau (3) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus ribu ringgit atau dipenjara selama tempoh tidak melebihi tiga tahun atau kedua-duanya.

BAHAGIAN IV

KETUA SEKTOR INFRASTRUKTUR MAKLUMAT KRITIKAL NEGARA DAN ENTITI INFRASTRUKTUR MAKLUMAT KRITIKAL NEGARA

Pelantikan ketua sektor infrastruktur maklumat kritikal negara

15. (1) Menteri boleh, atas syor Ketua Eksekutif, melantik mana-mana Entiti Kerajaan atau orang untuk menjadi ketua sektor infrastruktur maklumat kritikal negara bagi setiap sektor infrastruktur maklumat kritikal negara.

(2) Menteri boleh melantik lebih daripada satu ketua sektor infrastruktur maklumat kritikal negara bagi mana-mana sektor infrastruktur maklumat kritikal negara.

(3) Nama ketua sektor infrastruktur maklumat kritikal negara yang dilantik di bawah seksyen ini hendaklah disiarkan dalam laman sesawang rasmi Agensi Keselamatan Siber Negara.

Fungsi ketua sektor infrastruktur maklumat kritikal negara

16. Ketua sektor infrastruktur maklumat kritikal negara hendaklah, berkenaan dengan sektor infrastruktur maklumat kritikal negara yang baginya ia dilantik, mempunyai fungsi yang berikut:

- (a) untuk menetapkan suatu entiti infrastruktur maklumat kritikal negara di bawah seksyen 17;
- (b) untuk menyediakan suatu tataamalan sebagaimana yang dikehendaki di bawah seksyen 25;
- (c) untuk melaksanakan keputusan Jawatankuasa dan arahan di bawah Akta ini;
- (d) untuk mengawasi dan memastikan bahawa tindakan yang dikehendaki daripada dan kewajipan yang dikenakan ke atas entiti infrastruktur maklumat kritikal negara di bawah Akta ini dijalankan oleh entiti infrastruktur maklumat kritikal negara;
- (e) untuk menyediakan dan menyenggara garis panduan mengenai amalan terbaik berhubung dengan pengurusan keselamatan siber;
- (f) untuk menyediakan dan mengemukakan kepada Ketua Eksekutif suatu laporan situasi sama ada atas inisiatifnya sendiri atau sebagaimana yang dikehendaki oleh Ketua Eksekutif jika suatu ancaman keselamatan siber atau insiden keselamatan siber telah menjejaskan infrastruktur maklumat kritikal negara dalam sektor infrastruktur maklumat kritikal negaranya; dan
- (g) untuk menjalankan apa-apa fungsi lain di bawah Akta ini.

Penetapan entiti infrastruktur maklumat kritikal negara

17. (1) Ketua sektor infrastruktur maklumat kritikal negara boleh, berkenaan dengan sektor infrastruktur maklumat kritikal negara yang baginya ia dilantik, menetapkan mengikut cara sebagaimana yang ditentukan oleh Ketua Eksekutif, mana-mana Entiti Kerajaan atau orang sebagai entiti infrastruktur maklumat kritikal negara jika ketua sektor infrastruktur maklumat kritikal negara itu berpuas hati bahawa Entiti Kerajaan atau orang itu memiliki atau mengendalikan suatu infrastruktur maklumat kritikal negara.

(2) Bagi maksud subseksyen (1), ketua sektor infrastruktur maklumat kritikal negara boleh menghendaki Entiti Kerajaan atau orang itu untuk mengemukakan apa-apa maklumat, butir-butir atau dokumen sebagaimana yang ditentukan oleh ketua sektor infrastruktur maklumat kritikal negara itu termasuk maklumat yang berhubungan dengan fungsi dan reka bentuk komputer atau sistem komputer yang dimiliki atau dikendalikan oleh Entiti Kerajaan atau orang itu.

(3) Tiada Entiti Kerajaan boleh ditetapkan sebagai entiti infrastruktur maklumat kritikal negara oleh suatu ketua sektor infrastruktur maklumat kritikal negara yang bukan Entiti Kerajaan.

(4) Ketua sektor infrastruktur maklumat kritikal negara hendaklah memberitahu Ketua Eksekutif mengenai penetapan entiti infrastruktur maklumat kritikal negara yang dibuat di bawah subseksyen (1) bersama-sama dengan butir-butir yang berhubungan dengan infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu mengikut cara sebagaimana yang ditentukan oleh Ketua Eksekutif.

(5) Ketua sektor infrastruktur maklumat kritikal negara hendaklah menyimpan dan menyenggara suatu daftar entiti infrastruktur maklumat kritikal negara yang telah ditetapkan di bawah seksyen ini mengikut cara sebagaimana yang ditentukan oleh Ketua Eksekutif.

(6) Entiti infrastruktur maklumat kritikal negara yang telah ditetapkan di bawah seksyen ini hendaklah melalui notis secara bertulis memberitahu ketua sektor infrastruktur maklumat kritikal negaranya tanpa kelengahan jika—

- (a) entiti infrastruktur maklumat kritikal negara itu berpandangan bahawa komputer atau sistem komputer yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu bukan lagi merupakan suatu infrastruktur maklumat kritikal negara; atau

- (b) entiti infrastruktur maklumat kritikal negara itu tidak lagi memiliki atau mengendalikan apa-apa infrastruktur maklumat kritikal negara.

Penetapan ketua sektor infrastruktur maklumat kritikal negara sebagai entiti infrastruktur maklumat kritikal negara

18. (1) Ketua Eksekutif boleh menetapkan suatu ketua sektor infrastruktur maklumat kritikal negara sebagai entiti infrastruktur maklumat kritikal negara mengikut cara sebagaimana yang ditentukannya jika Ketua Eksekutif berpuas hati bahawa ketua sektor infrastruktur maklumat kritikal negara itu memiliki atau mengendalikan suatu infrastruktur maklumat kritikal negara.

(2) Bagi maksud subseksyen (1), Ketua Eksekutif boleh menghendaki ketua sektor infrastruktur maklumat kritikal negara itu untuk mengemukakan apa-apa maklumat, butir-butir atau dokumen sebagaimana yang ditentukan oleh Ketua Eksekutif termasuk maklumat yang berhubungan dengan fungsi dan reka bentuk komputer atau sistem komputer yang dimiliki atau dikendalikan oleh ketua sektor infrastruktur maklumat kritikal negara itu.

(3) Ketua Eksekutif hendaklah menyimpan dan menyenggara suatu daftar ketua sektor infrastruktur maklumat kritikal negara yang telah ditetapkan sebagai entiti infrastruktur maklumat kritikal negara di bawah seksyen ini mengikut cara sebagaimana yang ditentukan oleh Ketua Eksekutif.

(4) Ketua sektor infrastruktur maklumat kritikal negara yang telah ditetapkan sebagai entiti infrastruktur maklumat kritikal negara di bawah seksyen ini hendaklah melalui notis secara bertulis memberitahu Ketua Eksekutif tanpa kelengahan jika—

- (a) ketua sektor infrastruktur maklumat kritikal negara itu berpandangan bahawa komputer atau sistem komputer yang dimiliki atau dikendalikan oleh ketua sektor infrastruktur maklumat kritikal negara itu bukan lagi merupakan infrastruktur maklumat kritikal negara; atau
- (b) ketua sektor infrastruktur maklumat kritikal negara itu tidak lagi memiliki atau mengendalikan apa-apa infrastruktur maklumat kritikal negara.

Pembatalan penetapan entiti infrastruktur maklumat kritikal negara

19. (1) Ketua sektor infrastruktur maklumat kritikal negara boleh melalui notis secara bertulis kepada entiti infrastruktur maklumat kritikal negara, membatalkan penetapan entiti infrastruktur maklumat kritikal negara itu yang dibuat di bawah seksyen 17, jika ketua sektor infrastruktur maklumat kritikal negara berpuas hati bahawa entiti infrastruktur maklumat kritikal negara itu tidak lagi memiliki atau mengendalikan apa-apa infrastruktur maklumat kritikal negara.

(2) Pembatalan penetapan yang dibuat di bawah subseksyen (1) hendaklah berkuat kuasa dari tarikh yang dinyatakan dalam notis itu.

(3) Ketua sektor infrastruktur maklumat kritikal negara hendaklah memberitahu Ketua Eksekutif mengenai pembatalan yang dibuat di bawah subseksyen (1).

(4) Ketua Eksekutif boleh melalui notis secara bertulis kepada ketua sektor infrastruktur maklumat kritikal negara yang telah ditetapkan sebagai entiti infrastruktur maklumat kritikal negara di bawah seksyen 18, membatalkan penetapan ketua sektor infrastruktur maklumat kritikal negara itu jika Ketua Eksekutif berpuas hati bahawa ketua sektor infrastruktur maklumat kritikal negara itu tidak lagi memiliki atau mengendalikan apa-apa infrastruktur maklumat kritikal negara.

(5) Pembatalan penetapan yang dibuat di bawah subseksyen (4) hendaklah berkuat kuasa dari tarikh yang dinyatakan dalam notis itu dan tidaklah menjejaskan pelantikan ketua sektor infrastruktur maklumat kritikal negara itu di bawah seksyen 15.

Kewajipan untuk memberikan maklumat yang berhubungan dengan infrastruktur maklumat kritikal negara

20. (1) Ketua sektor infrastruktur maklumat kritikal negara boleh meminta suatu entiti infrastruktur maklumat kritikal negara berkenaan dengan sektor infrastruktur maklumat kritikal negara yang baginya ia dilantik untuk memberikan maklumat yang berhubungan dengan infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu

mengikuti cara sebagaimana yang ditentukan oleh ketua sektor infrastruktur maklumat kritikal negara itu dan entiti infrastruktur maklumat kritikal negara itu hendaklah mematuhi permintaan itu.

(2) Jika entiti infrastruktur maklumat kritikal negara itu memperoleh atau mempunyai dalam milikan atau kawalan apa-apa komputer atau sistem komputer tambahan yang pada pendapat entiti infrastruktur maklumat kritikal negara itu bahawa komputer atau sistem komputer itu merupakan suatu infrastruktur maklumat kritikal negara, entiti infrastruktur maklumat kritikal negara itu hendaklah memberikan maklumat itu kepada ketua sektor infrastruktur maklumat kritikal negaranya tidak kira sama ada terdapat permintaan di bawah subseksyen (1).

(3) Jika suatu perubahan material dibuat pada reka bentuk, konfigurasi, keselamatan atau pengendalian infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara selepas maklumat mengenai infrastruktur maklumat kritikal negara itu telah diberikan di bawah subseksyen (1), entiti infrastruktur maklumat kritikal negara itu hendaklah memberitahu ketua sektor infrastruktur maklumat kritikal negaranya mengenai perubahan material itu dalam masa tiga puluh hari dari tarikh perubahan itu selesai.

(4) Bagi maksud subseksyen (3), suatu perubahan ialah perubahan material jika perubahan itu menjejaskan atau boleh menjejaskan keselamatan siber infrastruktur maklumat kritikal negara itu atau keupayaan entiti infrastruktur maklumat kritikal negara itu untuk bertindak balas terhadap ancaman keselamatan siber atau insiden keselamatan siber.

(5) Ketua sektor infrastruktur maklumat kritikal negara hendaklah memberitahu Ketua Eksekutif mengenai apa-apa maklumat yang diterima di bawah subseksyen (2) dan (3) mengikut cara sebagaimana yang ditentukan oleh Ketua Eksekutif.

(6) Mana-mana entiti infrastruktur maklumat kritikal negara yang melanggar subseksyen (1), (2) atau (3) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

(7) Mana-mana ketua sektor infrastruktur maklumat kritikal negara yang melanggar subseksyen (5) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit.

Kewajipan untuk melaksanakan tataamalan

21. (1) Suatu entiti infrastruktur maklumat kritikal negara hendaklah melaksanakan langkah-langkah, standard dan proses sebagaimana yang dinyatakan dalam tataamalan untuk memastikan keselamatan siber infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu.

(2) Walau apa pun subseksyen (1), entiti infrastruktur maklumat kritikal negara boleh melaksanakan apa-apa langkah, standard dan proses alternatif jika entiti infrastruktur maklumat kritikal negara itu membuktikan sehingga memuaskan hati Ketua Eksekutif bahawa langkah-langkah, standard dan proses alternatif itu memberikan perlindungan yang sama atau lebih tinggi tahapnya kepada infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu.

(3) Suatu entiti infrastruktur maklumat kritikal negara boleh, sebagai tambahan kepada langkah-langkah, standard dan proses yang disebut dalam subseksyen (1) atau (2), mengadakan dan melaksanakan langkah-langkah, standard dan proses mengenai keselamatan siber berdasarkan standard atau rangka yang diiktiraf di peringkat antarabangsa.

(4) Jika suatu entiti infrastruktur maklumat kritikal negara melaksanakan langkah-langkah, standard dan proses untuk memastikan keselamatan siber infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikannya sebagaimana yang dikehendaki di bawah mana-mana undang-undang bertulis yang lain, entiti infrastruktur maklumat kritikal negara itu hendaklah disifatkan telah mematuhi seksyen ini dengan syarat bahawa langkah-langkah, standard dan proses itu tidak melanggar tataamalan.

(5) Mana-mana entiti infrastruktur maklumat kritikal negara yang melanggar subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi lima ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi sepuluh tahun atau kedua-duanya.

Kewajipan untuk membuat penilaian risiko keselamatan siber dan audit

22. (1) Suatu entiti infrastruktur maklumat kritikal negara hendaklah dalam tempoh sebagaimana yang ditetapkan—

- (a) membuat penilaian risiko keselamatan siber berkenaan dengan infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu mengikut tataamalan dan arahan; dan
- (b) menyebabkan suatu audit dijalankan oleh juruaudit yang diluluskan oleh Ketua Eksekutif untuk menentukan pematuhan entiti infrastruktur maklumat kritikal negara dengan Akta ini.

(2) Entiti infrastruktur maklumat kritikal negara hendaklah, dalam tempoh tiga puluh hari selepas penilaian risiko keselamatan siber atau audit di bawah subseksyen (1) selesai, mengemukakan laporan penilaian risiko keselamatan siber atau laporan audit itu kepada Ketua Eksekutif.

(3) Jika didapati oleh Ketua Eksekutif daripada laporan penilaian risiko keselamatan siber yang dikemukakan di bawah subseksyen (2) bahawa keputusan penilaian risiko keselamatan siber itu tidak memuaskan, Ketua Eksekutif boleh mengarahkan entiti infrastruktur maklumat kritikal negara untuk mengambil inisiatif selanjutnya untuk menilai semula risiko keselamatan siber terhadap infrastruktur maklumat kritikal negara itu dalam tempoh sebagaimana yang ditentukan oleh Ketua Eksekutif.

(4) Jika Ketua Eksekutif mendapati bahawa laporan audit yang dikemukakan di bawah subseksyen (2) tidak mencukupi, Ketua Eksekutif boleh mengarahkan entiti infrastruktur maklumat kritikal negara itu untuk membetulkan laporan audit itu dalam tempoh sebagaimana yang ditentukan oleh Ketua Eksekutif.

(5) Apabila menerima maklumat daripada ketua sektor infrastruktur maklumat kritikal negara di bawah subseksyen 20(5) mengenai perubahan material yang dibuat pada reka bentuk, konfigurasi, keselamatan atau pengendalian suatu infrastruktur maklumat kritikal negara, Ketua Eksekutif boleh melalui notis secara bertulis mengarahkan entiti infrastruktur maklumat kritikal negara yang memiliki atau mengendalikan infrastruktur maklumat kritikal negara itu untuk membuat penilaian risiko keselamatan siber atau menyebabkan dijalankan suatu audit berkenaan dengan infrastruktur maklumat kritikal negara itu tidak kira sama ada penilaian risiko keselamatan siber atau audit telah dibuat atau dijalankan di bawah subseksyen (1) berkenaan dengan infrastruktur maklumat kritikal negara itu.

(6) Ketua Eksekutif boleh mengarahkan suatu entiti infrastruktur maklumat kritikal negara untuk membuat penilaian risiko keselamatan siber atau menyebabkan dijalankan suatu audit sebagai tambahan kepada penilaian risiko keselamatan siber atau audit di bawah subseksyen (1) atau (5).

(7) Mana-mana entiti infrastruktur maklumat kritikal negara yang melanggar subseksyen (1) atau (2) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi tiga tahun atau kedua-duanya.

(8) Mana-mana entiti infrastruktur maklumat kritikal negara yang tidak mematuhi arahan Ketua Eksekutif di bawah subseksyen (3), (4), (5) atau (6) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit.

Kewajipan untuk memberikan pemberitahuan mengenai insiden keselamatan siber

23. (1) Jika sampai kepada pengetahuan suatu entiti infrastruktur maklumat kritikal negara bahawa suatu insiden keselamatan siber telah berlaku atau mungkin telah berlaku berkenaan dengan infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu, entiti infrastruktur maklumat kritikal negara itu hendaklah memberitahu Ketua Eksekutif dan ketua sektor infrastruktur maklumat kritikal negaranya mengenai maklumat itu dalam tempoh dan mengikut cara sebagaimana yang ditetapkan.

(2) Mana-mana entiti infrastruktur maklumat kritikal negara yang melanggar seksyen ini melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi lima ratus ribu ringgit atau dipenjara selama tempoh tidak melebihi sepuluh tahun atau kedua-duanya.

Latihan keselamatan siber

24. (1) Ketua Eksekutif boleh menjalankan suatu latihan keselamatan siber bagi maksud menilai kesediaan mana-mana entiti infrastruktur maklumat kritikal negara untuk bertindak balas terhadap apa-apa ancaman keselamatan siber atau insiden keselamatan siber.

(2) Ketua Eksekutif hendaklah, sebelum menjalankan apa-apa latihan keselamatan siber di bawah subseksyen (1), mengeluarkan notis secara bertulis kepada entiti infrastruktur maklumat kritikal negara yang berkenaan untuk memberitahu niatnya untuk menjalankan latihan keselamatan siber berkenaan dengan entiti infrastruktur maklumat kritikal negara itu.

(3) Ketua Eksekutif boleh memberikan apa-apa arahan kepada entiti infrastruktur maklumat kritikal negara sebagaimana yang Ketua Eksekutif fikirkan patut bagi maksud latihan keselamatan siber yang dijalankan di bawah seksyen ini.

(4) Mana-mana entiti infrastruktur maklumat kritikal negara yang tidak mematuhi arahan Ketua Eksekutif di bawah subseksyen (3) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit.

BAHAGIAN V

TATAAMALAN

Tataamalan

25. (1) Ketua sektor infrastruktur maklumat kritikal negara hendaklah menyediakan suatu tataamalan yang diendorskan oleh Ketua Eksekutif yang mengandungi langkah-langkah, standard dan proses dalam memastikan keselamatan siber suatu infrastruktur maklumat kritikal negara dalam sektor infrastruktur maklumat kritikal negara yang baginya ia dilantik.

(2) Ketua sektor infrastruktur maklumat kritikal negara hendaklah, dalam menyediakan tataamalan di bawah subseksyen (1), menimbangkan antara lain perkara yang berikut:

- (a) fungsi entiti infrastruktur maklumat kritikal negara yang berkaitan;
- (b) peruntukan yang berhubungan dengan keselamatan siber di bawah mana-mana undang-undang bertulis yang lain yang terpakai bagi ketua sektor infrastruktur maklumat kritikal negara itu;
- (c) pandangan entiti infrastruktur maklumat kritikal negara yang berkaitan; dan
- (d) pandangan pihak berkuasa kawal selia yang berkaitan, jika ada, yang kepadanya entiti infrastruktur maklumat kritikal negara tertakluk.

(3) Ketua Eksekutif boleh mengendorskan tataamalan yang disediakan di bawah subseksyen (1) jika Ketua Eksekutif berpuas hati bahawa—

- (a) langkah-langkah, standard dan proses yang dinyatakan dalam tataamalan adalah selaras dengan atau lebih tinggi daripada kehendak minimum yang dinyatakan dalam arahan;
- (b) perkara yang dinyatakan dalam subseksyen (2) telah diberikan pertimbangan yang sewajarnya; dan
- (c) tataamalan itu adalah selaras dengan peruntukan Akta ini.

(4) Tataamalan di bawah seksyen ini hendaklah berkuat kuasa pada tarikh pengendorsan tataamalan oleh Ketua Eksekutif.

(5) Jika Ketua Eksekutif enggan mengendorskan tataamalan itu, Ketua Eksekutif hendaklah memberitahu ketua sektor infrastruktur maklumat kritikal negara yang berkenaan mengenai keputusannya secara bertulis dan memberikan sebab bagi keputusannya.

(6) Mana-mana ketua sektor infrastruktur maklumat kritikal negara yang melanggar subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi seratus ribu ringgit.

Arahan di bawah undang-undang bertulis yang lain hendaklah selaras dengan tataamalan

26. Jika ketua sektor infrastruktur maklumat kritikal negara mengarahkan mana-mana entiti infrastruktur maklumat kritikal negara untuk melaksanakan langkah-langkah, standard dan proses untuk memastikan keselamatan siber infrastruktur maklumat kritikal negara yang dimiliki atau dikendalikan oleh entiti infrastruktur maklumat kritikal negara itu di bawah mana-mana undang-undang bertulis yang lain, ketua sektor infrastruktur maklumat kritikal negara itu hendaklah memastikan bahawa arahan yang diberikan itu adalah selaras dengan tataamalan.

BAHAGIAN VI

PEMBERI PERKHIDMATAN KESELAMATAN SIBER

Pelesenan pemberi perkhidmatan keselamatan siber

27. (1) Tiada seorang pun boleh—

- (a) memberikan apa-apa perkhidmatan keselamatan siber; atau
- (b) mengiklankan, atau dalam apa-apa cara mengemukakan dirinya sebagai pemberi suatu perkhidmatan keselamatan siber,

melainkan jika dia memegang suatu lesen untuk memberikan perkhidmatan keselamatan siber yang dikeluarkan di bawah Bahagian ini.

(2) Menteri boleh menetapkan apa-apa perkhidmatan keselamatan siber yang berkenaan dengannya suatu lesen hendaklah diperoleh di bawah Bahagian ini.

(3) Bahagian ini tidak terpakai dalam hal jika perkhidmatan keselamatan siber diberikan oleh suatu syarikat kepada syarikat berkaitannya.

(4) Dalam seksyen ini, “syarikat berkaitan” mempunyai erti yang diberikan kepadanya di bawah Akta Syarikat 2016 [*Akta 777*].

(5) Mana-mana orang yang melanggar subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi lima ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi sepuluh tahun atau kedua-duanya.

Kelayakan bagi permohonan lesen

28. Mana-mana orang boleh memohon bagi suatu lesen di bawah Bahagian ini jika orang itu—

- (a) memenuhi kehendak prasyarat sebagaimana yang ditentukan oleh Ketua Eksekutif; dan
- (b) tidak pernah disabitkan atas suatu kesalahan yang melibatkan fraud, kecurangan atau keburukan akhlak.

Permohonan bagi lesen

29. (1) Suatu permohonan bagi lesen untuk memberikan perkhidmatan keselamatan siber hendaklah dibuat kepada Ketua Eksekutif mengikut cara sebagaimana yang ditetapkan.

(2) Permohonan di bawah subseksyen (1) hendaklah disertakan dengan pembayaran fi yang ditetapkan dan apa-apa maklumat, butir-butir atau dokumen sebagaimana yang ditentukan oleh Ketua Eksekutif.

(3) Selepas mempertimbangkan permohonan itu, Ketua Eksekutif boleh—

- (a) meluluskan permohonan itu dan mengeluarkan kepada pemohon selepas dibayar fi yang ditetapkan suatu lesen dalam bentuk sebagaimana yang ditentukan oleh Ketua Eksekutif; atau
- (b) menolak permohonan itu, dengan menyatakan alasan bagi penolakan itu.

(4) Suatu lesen yang dikeluarkan di bawah seksyen ini adalah sah bagi suatu tempoh sebagaimana yang dinyatakan dalam lesen itu.

Pembaharuan lesen

30. (1) Pemegang lesen boleh memohon untuk membaharui lesennya yang dikeluarkan di bawah seksyen 29 sekurang-kurangnya tiga puluh hari sebelum tarikh luput lesen itu mengikut cara sebagaimana yang ditetapkan.

(2) Permohonan di bawah subseksyen (1) hendaklah disertakan dengan pembayaran fi yang ditetapkan dan apa-apa maklumat, butir-butir atau dokumen sebagaimana yang ditentukan oleh Ketua Eksekutif.

(3) Selepas mempertimbangkan permohonan itu, Ketua Eksekutif boleh—

- (a) meluluskan permohonan itu dan membaharui lesen itu apabila fi yang ditetapkan dibayar; atau
- (b) menolak permohonan itu, dengan menyatakan alasan bagi penolakan itu.

Syarat lesen

31. (1) Suatu lesen untuk memberikan perkhidmatan keselamatan siber boleh dikeluarkan tertakluk kepada apa-apa syarat sebagaimana yang Ketua Eksekutif fikirkan patut dikenakan.

(2) Ketua Eksekutif boleh pada bila-bila masa mengubah atau membatalkan syarat yang dikenakan ke atas suatu lesen di bawah subseksyen (1).

(3) Mana-mana orang yang melanggar mana-mana syarat lesen yang dikenakan di bawah subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

Kewajipan untuk menyimpan dan menyenggara rekod

32. (1) Pemegang lesen hendaklah, bagi setiap kali pemegang lesen itu diambil khidmat untuk memberikan perkhidmatan keselamatan siber, menyimpan dan menyenggara rekod yang berikut:

- (a) nama dan alamat orang yang mengambil khidmat pemegang lesen bagi perkhidmatan keselamatan siber;

- (b) nama orang yang memberikan perkhidmatan keselamatan siber bagi pihak pemegang lesen itu, jika ada;
 - (c) tarikh dan masa perkhidmatan keselamatan siber yang telah diberikan oleh pemegang lesen atau oleh orang lain bagi pihak pemegang lesen;
 - (d) butiran mengenai jenis perkhidmatan keselamatan siber yang diberikan; dan
 - (e) apa-apa butir lain sebagaimana yang ditentukan oleh Ketua Eksekutif.
- (2) Maklumat yang dirujuk dalam subseksyen (1) hendaklah—
- (a) disimpan dan disenggara mengikut cara yang ditentukan oleh Ketua Eksekutif;
 - (b) dipegang simpan bagi suatu tempoh tidak kurang dari enam tahun dari tarikh perkhidmatan keselamatan siber diberikan; dan
 - (c) dikemukakan kepada Ketua Eksekutif pada bila-bila masa sebagaimana yang diarahkan oleh Ketua Eksekutif.
- (3) Mana-mana orang yang melanggar subseksyen (1) atau (2) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

Pembatalan atau penggantungan lesen

33. Ketua Eksekutif boleh membatalkan atau menggantung lesen yang dikeluarkan di bawah seksyen 29 jika Ketua Eksekutif berpuas hati bahawa—

- (a) pemegang lesen telah tidak mematuhi mana-mana syarat lesen;
- (b) lesen itu telah diperolehi dengan cara fraud atau salah nyataan;

- (c) suatu hal keadaan wujud pada masa lesen itu dikeluarkan atau dibaharui yang tidak disedari oleh Ketua Eksekutif, yang mungkin akan menyebabkan Ketua Eksekutif enggan mengeluarkan atau membaharui lesen itu jika Ketua Eksekutif menyedari hal keadaan itu pada masa itu;
- (d) pemegang lesen telah berhenti daripada menjalankan perniagaan yang berkenaan dengannya pemegang lesen itu dilesenkan di bawah Akta ini;
- (e) pemegang lesen telah dihukum bankrap atau berada dalam penyelesaian atau sedang digulungkan;
- (f) pemegang lesen telah disabitkan atas kesalahan di bawah Akta ini atau kesalahan yang melibatkan fraud, kecurangan atau keburukan akhlak; atau
- (g) pembatalan atau penggantungan itu adalah demi kepentingan awam atau keselamatan negara.

Pemindahmilikan atau penyerahhakan lesen

34. (1) Suatu lesen tidak boleh dipindahmilikkan atau diserahkan kepada mana-mana orang lain.

(2) Mana-mana orang yang melanggar subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi tiga tahun atau kedua-duanya.

(3) Walau apa pun subseksyen (1), suatu lesen boleh dipindahmilikkan kepada mana-mana orang lain dengan kelulusan Ketua Eksekutif—

- (a) jika suatu permohonan secara bertulis dibuat kepada Ketua Eksekutif oleh pemegang lesen; dan
- (b) jika Ketua Eksekutif berpuas hati bahawa orang yang kepadanya lesen itu hendak dipindahmilikkan mempunyai sumber kewangan dan teknikal yang perlu untuk mematuhi syarat lesen itu.

BAHAGIAN VII

INSIDEN KESELAMATAN SIBER

Insiden keselamatan siber

35. (1) Apabila diterima pemberitahuan mengenai insiden keselamatan siber daripada entiti infrastruktur maklumat kritikal negara di bawah seksyen 23 atau jika sampai kepada pengetahuan Ketua Eksekutif bahawa insiden keselamatan siber berkenaan dengan suatu infrastruktur maklumat kritikal negara telah atau mungkin telah berlaku, Ketua Eksekutif hendaklah mengarahkan pegawai diberi kuasa untuk menyiasat perkara itu.

(2) Siasatan yang dijalankan di bawah Bahagian ini hendaklah bagi maksud—

- (a) menentukan sama ada suatu insiden keselamatan siber telah berlaku; atau
- (b) dalam hal jika insiden keselamatan siber telah berlaku, menentukan langkah-langkah yang perlu untuk bertindak balas terhadap atau pulih daripada insiden keselamatan siber itu dan mencegah insiden keselamatan siber itu daripada berlaku pada masa hadapan.

(3) Apabila siasatan oleh pegawai diberi kuasa di bawah Bahagian ini selesai—

- (a) jika pegawai diberi kuasa mendapati bahawa tiada insiden keselamatan siber telah berlaku, pegawai diberi kuasa hendaklah memberitahu Ketua Eksekutif mengenai hasil dapatannya dan Ketua Eksekutif hendaklah memberitahu entiti infrastruktur maklumat kritikal negara yang memiliki atau mengendalikan infrastruktur maklumat kritikal negara yang disebut dalam subseksyen (1) dengan sewajarnya dan menggugurkan perkara itu; atau
- (b) jika pegawai diberi kuasa mendapati bahawa suatu insiden keselamatan siber telah berlaku, pegawai diberi kuasa hendaklah memberitahu Ketua Eksekutif mengenai hasil dapatannya dan Ketua Eksekutif hendaklah memberitahu entiti infrastruktur maklumat kritikal negara yang memiliki atau mengendalikan infrastruktur maklumat kritikal negara yang disebut dalam subseksyen (1) dengan sewajarnya.

(4) Setelah diberitahu oleh pegawai diberi kuasa di bawah perenggan (3)(b) bahawa suatu insiden keselamatan siber telah berlaku, Ketua Eksekutif boleh mengeluarkan arahan kepada entiti infrastruktur maklumat kritikal negara yang memiliki atau mengendalikan infrastruktur maklumat kritikal negara yang berkenaan mengenai langkah-langkah yang perlu untuk bertindak balas terhadap atau pulih daripada insiden keselamatan siber itu dan untuk mencegah insiden keselamatan siber itu daripada berlaku pada masa hadapan.

(5) Mana-mana entiti infrastruktur maklumat kritikal negara yang tidak mematuhi arahan Ketua Eksekutif di bawah subseksyen (4) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi dua ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi tiga tahun atau kedua-duanya.

BAHAGIAN VIII

PENGUATKUASAAN

Pemberikuasaan pegawai awam

36. Menteri boleh, secara bertulis, memberi kuasa kepada mana-mana pegawai awam untuk menjalankan kuasa penguatkuasaan di bawah Akta ini.

Kad kuasa

37. (1) Maka hendaklah dikeluarkan kepada setiap pegawai diberi kuasa suatu kad kuasa yang ditandatangani oleh Menteri.

(2) Bilamana pegawai diberi kuasa itu menjalankan mana-mana kuasa di bawah Akta ini, pegawai diberi kuasa itu hendaklah, apabila diminta, mengemukakan kepada orang yang terhadapnya kuasa itu sedang dijalankan kad kuasa yang dikeluarkan kepadanya di bawah subseksyen (1).

Kuasa penyiasatan

38. (1) Seseorang pegawai diberi kuasa hendaklah mempunyai segala kuasa yang perlu untuk menjalankan penyiasatan berhubung dengan apa-apa insiden keselamatan siber di bawah Akta ini.

(2) Seorang pegawai diberi kuasa hendaklah mempunyai kuasa seorang pegawai polis yang apa jua pun pangkatnya sebagaimana yang diperuntukkan di bawah Kanun Tatacara Jenayah [Akta 593] berhubung dengan penyiasatan apa-apa kesalahan di bawah Akta ini, dan kuasa itu hendaklah sebagai tambahan dan bukan pengurangan bagi, kuasa yang diperuntukkan di bawah Akta ini.

Pengeledahan dan penyitaan dengan waran

39. (1) Jika ternyata pada seseorang Majistret, berdasarkan maklumat bertulis dengan bersumpah daripada pegawai diberi kuasa dan selepas apa-apa siasatan sebagaimana yang difikirkan perlu oleh Majistret itu, bahawa terdapat sebab yang munasabah untuk mempercayai bahawa—

- (a) mana-mana premis telah digunakan dalam; atau
- (b) terdapat di dalam mana-mana premis keterangan yang perlu untuk menjalankan suatu penyiasatan,

perlakuan suatu kesalahan di bawah Akta ini, Majistret boleh mengeluarkan suatu waran yang memberikan kuasa kepada pegawai diberi kuasa yang dinamakan dalam waran itu, pada bila-bila masa yang munasabah pada waktu siang atau malam dan dengan atau tanpa bantuan, untuk memasuki premis itu dan jika perlu dengan menggunakan kekerasan.

(2) Tanpa menjejaskan keluasan subseksyen (1), waran yang dikeluarkan oleh Majistret boleh memberi kuasa untuk pengeledahan dan penyitaan—

- (a) salinan mana-mana buku, akaun atau dokumen lain, termasuk data berkomputer, yang mengandungi atau yang semunasabahnya disyaki mengandungi maklumat mengenai apa-apa kesalahan yang disyaki telah dilakukan;
- (b) mana-mana papan tanda, kad, surat, risalah, lembaran atau notis yang menyatakan atau membayangkan bahawa orang itu mempunyai suatu lesen yang diberikan di bawah Akta ini; atau

- (c) apa-apa dokumen, kemudahan, radas, kenderaan, kelengkapan, peranti atau bahan lain yang semunasabahnya dipercayai dapat memberikan keterangan mengenai pelakuan kesalahan itu.

(3) Seorang pegawai diberi kuasa yang membuat penggeledahan di bawah subseksyen (1) boleh, bagi maksud menyiasat kesalahan itu, memeriksa mana-mana orang yang berada di dalam atau di premis itu.

(4) Seorang pegawai diberi kuasa yang membuat pemeriksaan terhadap seseorang di bawah subseksyen (3) boleh menyita atau mengambil milik, dan menyimpan dalam jagaan selamat semua benda, selain pakaian yang perlu dipakai, yang dijumpai pada orang itu, dan apa-apa benda lain, yang baginya ada sebab untuk dipercayai bahawa benda-benda itu merupakan peralatan atau keterangan lain bagi jenayah itu, dan benda-benda itu boleh ditahan sehingga orang itu dilepaskan atau dibebaskan.

(5) Tiada seorang pun boleh diperiksa kecuali oleh seorang lain yang sama jantina, dan pemeriksaan sedemikian hendaklah dibuat dengan penuh kesopanan.

(6) Jika, oleh sebab sifat, saiz atau amaunnya, pemindahan mana-mana objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disita di bawah seksyen ini tidak boleh dilaksanakan, pegawai yang menyita hendaklah, dengan apa-apa cara, mengelak objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu di dalam atau di premis yang di dalamnya ia dijumpai.

(7) Mana-mana orang yang, tanpa kuasa yang sah, memecahkan, mengusik atau merosakkan lak yang disebut dalam subseksyen (6) atau mengalihkan mana-mana objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang dilak atau cuba untuk berbuat demikian melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

Pengeledahan dan penyitaan tanpa waran

40. Jika seseorang pegawai diberi kuasa berpuas hati atas maklumat yang diterima bahawa dia mempunyai sebab yang munasabah untuk mempercayai bahawa oleh sebab kelengahan dalam memperoleh waran geledah di bawah seksyen 39 penyiasatan akan terjejas atau keterangan mengenai pelakuan sesuatu kesalahan mungkin diganggu, dipindahkan, dirosakkan atau dimusnahkan, pegawai diberi kuasa itu boleh memasuki premis itu dan menjalankan di dalam, pada dan berkenaan dengan premis itu semua kuasa yang disebut dalam seksyen 39 dengan cara yang sepenuhnya dan secukupnya seolah-olah dia diberi kuasa untuk berbuat demikian oleh suatu waran yang dikeluarkan di bawah seksyen itu.

Senarai objek, dsb., yang disita

41. (1) Jika apa-apa penyitaan dibuat di bawah Akta ini, pegawai diberi kuasa yang membuat penyitaan itu hendaklah menyediakan suatu senarai objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disita dan hendaklah menandatangani senarai itu.

(2) Senarai yang disediakan mengikut subseksyen (1) hendaklah diserahkan dengan serta-merta kepada pemunya atau orang yang mengawal atau menjaga premis yang telah digeledah, atau kepada ejen atau pekerja pemunya atau orang itu, di premis itu.

Kos memegang objek, dsb., yang disita

42. Jika apa-apa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disita di bawah Akta ini dipegang dalam jagaan Kerajaan Persekutuan sementara menunggu penyelesaian apa-apa prosiding yang berkenaan dengan suatu kesalahan di bawah Akta ini, kos bagi memegangnya dalam jagaan hendaklah, sekiranya mana-mana orang telah disabitkan atas kesalahan itu, menjadi hutang yang kena dibayar kepada Kerajaan Persekutuan oleh orang itu dan hendaklah didapatkan kembali dengan sewajarnya.

Pelepasan objek, dsb., yang disita

43. (1) Jika apa-apa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan telah disita di bawah Akta ini, mana-mana pegawai diberi kuasa, boleh pada bila-bila masa, selepas merujuk kepada Timbalan Pendakwa Raya, melepaskan objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu kepada orang yang ditentukannya sebagai berhak secara sah kepada objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu jika dia berpuas hati bahawa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu tidak boleh dilucuthakkan di bawah Akta ini dan tidak dikehendaki selainnya bagi maksud mana-mana prosiding di bawah Akta ini, atau bagi maksud apa-apa pendakwaan di bawah mana-mana undang-undang bertulis yang lain, dan dalam hal sedemikian baik pegawai diberi kuasa yang membuat penyitaan itu, mahupun Kerajaan Persekutuan atau mana-mana orang yang bertindak bagi pihak Kerajaan Persekutuan, tidak boleh dikenakan apa-apa prosiding oleh mana-mana orang jika penyitaan dan pelepasan objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu telah dibuat dengan suci hati.

(2) Suatu rekod secara bertulis hendaklah dibuat oleh pegawai diberi kuasa yang membuat pelepasan objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan di bawah subseksyen (1) yang menyatakan secara terperinci hal keadaan dan sebab bagi pelepasan itu, dan dia hendaklah menghantarkan suatu salinan rekod itu kepada Timbalan Pendakwa Raya dengan seberapa segera yang boleh praktik.

Pelucuthakan objek, dsb., yang disita

44. (1) Apa-apa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang

disita dalam perjalanan mana-mana kuasa yang diberikan di bawah Akta ini boleh dilucuthakkan.

(2) Suatu perintah bagi pelucuthakan mana-mana objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu hendaklah dibuat jika dibuktikan sehingga memuaskan hati mahkamah bahawa suatu kesalahan di bawah Akta ini telah dilakukan dan bahawa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu adalah hal perkara atau telah digunakan dalam pelakuan kesalahan itu, walaupun tiada seorang pun telah disabitkan atas kesalahan itu.

(3) Jika tiada pendakwaan berkenaan dengan apa-apa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disita di bawah Akta ini, objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu hendaklah dikira dan disifatkan terlucut hak apabila habis tempoh satu bulan kalendar dari tarikh penyampaian notis kepada alamat yang terakhir diketahui orang yang daripadanya objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu telah disita yang menyatakan bahawa tidak ada pendakwaan berkenaan dengan objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu melainkan jika sebelum habis tempoh itu suatu tuntutan baginya telah dibuat mengikut cara yang dinyatakan dalam subseksyen (4), (5), (6) dan (7).

(4) Mana-mana orang yang menegaskan bahawa dia ialah pemunya objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disebut dalam subseksyen (3) dan bahawa ia tidak boleh dilucuthakkan boleh secara sendiri atau melalui ejennya yang diberi kuasa secara bertulis, memberikan notis bertulis kepada pegawai diberi kuasa yang dalam milikannya objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis,

kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu dipegang bahawa dia menuntut objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu.

(5) Apabila notis yang disebut dalam subseksyen (4) diterima, pegawai diberi kuasa itu hendaklah merujuk tuntutan itu kepada seorang Majistret bagi keputusannya.

(6) Majistret yang kepadanya sesuatu perkara dirujuk di bawah subseksyen (5) hendaklah mengeluarkan suatu saman yang menghendaki orang yang menegaskan bahawa dia ialah pemunya objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu dan orang yang daripadanya ia disita untuk hadir di hadapannya, dan apabila mereka hadir atau mereka tidak hadir, setelah dibuktikan bahawa saman itu telah disampaikan dengan sewajarnya, Majistret itu hendaklah meneruskan pemeriksaan perkara itu.

(7) Jika dibuktikan bahawa suatu kesalahan di bawah Akta ini telah dilakukan dan bahawa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disebut dalam subseksyen (6) ialah hal perkara bagi atau telah digunakan dalam pelakuan kesalahan itu, Majistret itu hendaklah memerintahkan supaya objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan itu dilucuthakkan, dan hendaklah, jika tiada bukti sedemikian, memerintahkan pelepasannya.

(8) Mana-mana objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang dilucuthakkan atau disifatkan terlucut hak hendaklah diserahkan kepada Ketua Eksekutif dan hendaklah dilupuskan dalam apa-apa cara sebagaimana yang difikirkan patut oleh Ketua Eksekutif.

Hak harta mengenai objek, dsb., yang dilucuthakkan

45. Apa-apa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang dilucuthakkan atau disifatkan terlucut hak di bawah Akta ini hendaklah menjadi harta Kerajaan Persekutuan.

Akses kepada data berkomputer

46. (1) Mana-mana pegawai diberi kuasa yang membuat pengeledahan di bawah Akta ini hendaklah diberikan akses kepada data berkomputer sama ada disimpan dalam suatu komputer atau selainnya.

(2) Bagi maksud seksyen ini, pegawai diberi kuasa hendaklah diberikan kata laluan, kod penyulitan, kod penyahsulitan, perisian atau perkakasan yang perlu dan apa-apa cara lain yang dikehendaki untuk membolehkan data berkomputer itu difahami.

Tiada kos atau ganti rugi yang berbangkit daripada penyitaan boleh didapatkan

47. Tiada seorang pun boleh, dalam apa-apa prosiding di hadapan mana-mana mahkamah berkenaan dengan apa-apa objek, buku, akaun, dokumen, data berkomputer, papan tanda, kad, surat, risalah, lembaran, notis, kemudahan, radas, kenderaan, kelengkapan, peranti, benda atau bahan yang disita dalam menjalankan atau yang berupa sebagai menjalankan mana-mana kuasa yang diberikan di bawah Akta ini, berhak kepada kos prosiding itu atau apa-apa ganti rugi atau relief lain melainkan jika penyitaan itu dibuat tanpa sebab yang munasabah.

Kuasa untuk menghendaki kehadiran orang yang mempunyai pengetahuan tentang kes

48. (1) Seorang pegawai diberi kuasa yang membuat suatu penyiasatan di bawah Bahagian ini boleh, melalui perintah secara bertulis, menghendaki mana-mana orang yang pada pendapat pegawai diberi kuasa itu mempunyai pengetahuan tentang fakta dan hal keadaan kes itu supaya hadir di hadapannya, dan orang itu hendaklah hadir sebagaimana yang dikehendaki.

(2) Jika mana-mana orang enggan atau tidak hadir sebagaimana yang dikehendaki oleh suatu perintah yang dibuat di bawah subseksyen (1), pegawai diberi kuasa itu boleh melaporkan keengganan atau ketidakhadiran itu kepada Majistret yang hendaklah mengeluarkan suatu waran untuk memastikan kehadiran orang itu sebagaimana yang dikehendaki oleh perintah itu.

Pemeriksaan orang yang mempunyai pengetahuan tentang kes

49. (1) Seorang pegawai diberi kuasa yang membuat suatu penyiasatan di bawah Akta ini boleh memeriksa secara lisan mana-mana orang yang dikatakan mempunyai pengetahuan tentang fakta dan hal keadaan kes itu.

(2) Orang itu adalah terikat untuk menjawab segala soalan yang berhubungan dengan kes itu yang dikemukakan kepadanya oleh pegawai diberi kuasa itu, tetapi dia boleh enggan menjawab apa-apa soalan yang jawapannya mungkin mendedahkannya kepada suatu pertuduhan jenayah atau penalti atau pelucuthakan.

(3) Seorang yang membuat pernyataan di bawah seksyen ini adalah terikat di sisi undang-undang untuk menyatakan yang benar, sama ada pernyataan itu dibuat keseluruhannya atau sebahagiannya bagi menjawab soalan-soalan atau tidak.

(4) Pegawai diberi kuasa yang memeriksa seseorang di bawah subseksyen (1) hendaklah terlebih dahulu memaklumkan orang itu mengenai peruntukan subseksyen (2) dan (3).

(5) Suatu pernyataan yang dibuat oleh mana-mana orang di bawah seksyen ini hendaklah, bilamana mungkin, diubah ke dalam bentuk bertulis dan ditandatangani oleh orang yang membuatnya atau dilekatkan dengan cap jarinya, mengikut mana-mana yang berkenaan—

- (a) selepas pernyataan itu dibacakan kepadanya dalam bahasa yang dalamnya pernyataan itu dibuat olehnya; dan
- (b) selepas dia diberi peluang untuk membuat apa-apa pembedulan yang ingin dibuat olehnya.

Kebolehterimaan pernyataan sebagai keterangan

50. (1) Kecuali sebagaimana yang diperuntukkan dalam seksyen ini, tiada pernyataan yang dibuat oleh mana-mana orang kepada pegawai diberi kuasa dalam penjalanan suatu penyiasatan yang dibuat di bawah Akta ini boleh digunakan sebagai keterangan.

(2) Apabila mana-mana saksi dipanggil bagi pendakwaan atau bagi pembelaan, selain tertuduh, mahkamah hendaklah, atas permintaan orang tertuduh atau pendakwa, merujuk kepada mana-mana pernyataan yang dibuat oleh saksi itu kepada pegawai diberi kuasa dalam penjalanan penyiasatan di bawah Akta ini dan boleh kemudian, jika mahkamah fikirkan patut demi kepentingan keadilan, mengarahkan supaya tertuduh diberikan suatu salinan pernyataan itu dan pernyataan itu boleh digunakan untuk mencabar kebolehpercayaan saksi itu mengikut cara yang diperuntukkan oleh Akta Keterangan 1950 [*Akta 56*].

(3) Jika tertuduh telah membuat suatu pernyataan semasa penjalanan suatu penyiasatan, pernyataan itu boleh diterima sebagai keterangan untuk menyokong pembelaannya semasa penjalanan perbicaraan.

(4) Tiada apa-apa jua dalam seksyen ini boleh disifatkan terpakai bagi apa-apa pernyataan yang dibuat dalam penjalanan suatu kawad cam atau tergolong dalam seksyen 27 atau perenggan 32(1)(a), (i) dan (j) Akta Keterangan 1950.

(5) Apabila mana-mana orang dipertuduh atas mana-mana kesalahan berhubung dengan pembuatan atau kandungan apa-apa pernyataan yang dibuat olehnya kepada seorang pegawai diberi kuasa dalam penjalanan suatu penyiasatan yang dibuat di bawah Akta ini, pernyataan itu boleh digunakan sebagai keterangan dalam kes pendakwaan.

Kuasa tambahan

51. (1) Seorang pegawai diberi kuasa hendaklah, bagi maksud melaksanakan Akta ini, mempunyai kuasa untuk melakukan segala atau mana-mana daripada perkara yang berikut:

- (a) menghendaki pengemukaan apa-apa komputer, buku, rekod, data berkomputer, dokumen atau benda lain dan untuk meneliti, memeriksa dan menyalin apa-apa daripadanya;

- (b) menghendaki pengemukaan apa-apa dokumen pengenalan daripada mana-mana orang berhubung dengan mana-mana perbuatan atau kesalahan di bawah Akta ini; dan
- (c) membuat apa-apa siasatan sebagaimana yang perlu untuk menentukan sama ada peruntukan Akta ini telah dipatuhi.

(2) Mana-mana orang yang tidak mematuhi kehendak yang dibuat di bawah subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

Halangan

52. Mana-mana orang yang mengamang, menghalang, merintang atau mengganggu, atau enggan memberikan akses ke mana-mana premis atau data berkomputer kepada, Ketua Eksekutif atau pegawai diberi kuasa dalam pelaksanaan kewajipannya di bawah Akta ini melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

BAHAGIAN IX

AM

Rayuan

53. (1) Mana-mana orang yang terkilan—

- (a) dengan keengganan Ketua Eksekutif untuk mengeluarkan kepadanya suatu lesen di bawah Akta ini; atau
- (b) dengan pembatalan atau penggantungan lesennya,

boleh, dalam masa tiga puluh hari selepas dimaklumkan secara bertulis mengenai keengganan, pembatalan atau penggantungan itu, membuat rayuan secara bertulis terhadap keputusan itu kepada Menteri.

(2) Menteri boleh, selepas mempertimbangkan rayuan yang dibuat di bawah subseksyen (1), mengesahkan atau mengetepikan keputusan yang dirayukan itu.

Penyampaian dokumen

54. (1) Tertakluk kepada subseksyen (2), Ketua Eksekutif boleh membenarkan apa-apa maklumat, butir-butir atau dokumen yang dikehendaki untuk dikemukakan atau diberikan di bawah Akta ini supaya dikemukakan atau diberikan melalui media elektronik atau secara penghantaran elektronik.

(2) Syarat dan spesifikasi yang di bawahnya maklumat, butir-butir atau dokumen yang disebut dalam subseksyen (1) dikemukakan atau diberikan hendaklah sebagaimana yang ditentukan oleh Ketua Eksekutif.

(3) Maklumat, butir-butir atau dokumen yang disebut dalam subseksyen (1) hendaklah disifatkan telah dikemukakan atau diberikan oleh seseorang kepada Ketua Eksekutif pada tarikh pengakuteraan dokumen itu dihantar secara elektronik oleh Ketua Eksekutif kepada orang itu.

(4) Pengakuteraan oleh Ketua Eksekutif mengenai maklumat, butir-butir atau dokumen yang dikemukakan atau diberikan menurut subseksyen (3) boleh diterima sebagai keterangan dalam mana-mana prosiding.

Kewajipan kerahsiaan

55. (1) Kecuali bagi apa-apa maksud Akta ini atau bagi maksud apa-apa prosiding sivil atau jenayah di bawah mana-mana undang-undang bertulis atau jika selainnya dibenarkan oleh Jawatankuasa, mana-mana anggota Jawatankuasa, Ketua Eksekutif atau mana-mana pegawai diberi kuasa, sama ada semasa atau selepas tempoh jawatan atau pekerjaannya, tidak boleh menzahirkan apa-apa maklumat yang diperolehnya semasa melaksanakan kewajipannya.

(2) Mana-mana orang yang melanggar subseksyen (1) melakukan suatu kesalahan dan boleh, apabila disabitkan, didenda tidak melebihi satu ratus ribu ringgit atau dipenjarakan selama tempoh tidak melebihi dua tahun atau kedua-duanya.

Perlindungan daripada guaman dan prosiding undang-undang

56. Tiada tindakan, guaman, pendakwaan atau prosiding lain boleh dibawa, dimulakan atau dikekalkan dalam mana-mana mahkamah terhadap Menteri, mana-mana anggota Jawatankuasa, Ketua Eksekutif atau mana-mana pegawai diberi kuasa atas sebab atau yang berkenaan dengan apa-apa perbuatan, kecuaiian atau keingkaran yang dilakukan atau ditinggalkan olehnya dalam masa menjalankan kewajibannya di bawah Akta ini melainkan jika boleh dibuktikan bahawa perbuatan, kecuaiian atau keingkaran telah dilakukan atau ditinggalkan dengan niat jahat dan tanpa sebab yang munasabah.

Pendakwaan

57. Tiada pendakwaan bagi suatu kesalahan di bawah Akta ini boleh dimulakan kecuali oleh atau dengan keizinan bertulis Pendakwa Raya.

Tanggungan pengarah, dsb., bagi syarikat, dsb.

58. Jika mana-mana orang yang melakukan kesalahan di bawah Akta ini ialah suatu syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain, seseorang yang pada masa pelakuan kesalahan itu ialah seorang pengarah, pegawai pematuhan, pekongsi, pengurus, setiausaha atau pegawai lain yang seumpamanya bagi syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain itu atau yang berupa sebagai bertindak atas sifat itu atau yang dengan apa-apa cara atau sehingga apa-apa takat bertanggungjawab bagi pengurusan apa-apa hal ehwal syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain itu atau yang membantu dalam pengurusannya—

- (a) boleh dipertuduh secara berasingan atau berseksama dalam prosiding yang sama bersekali dengan syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain itu; dan
- (b) jika syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain itu didapati bersalah atas kesalahan itu, hendaklah disifatkan bersalah atas

kesalahan itu dan boleh dikenakan hukuman atau penalti yang sama sebagaimana seorang individu melainkan jika, dengan mengambil kira jenis fungsinya atas sifat itu dan segala hal keadaan, dia membuktikan—

- (i) bahawa kesalahan itu telah dilakukan tanpa pengetahuannya; dan
- (ii) bahawa kesalahan itu telah dilakukan tanpa persetujuan atau pembiarannya dan bahawa dia telah mengambil segala langkah yang munasabah dan menjalankan usaha yang wajar untuk menghalang pelakuan kesalahan itu.

Tanggungjawab seseorang bagi perbuatan, dsb., pekerja, dsb.

59. Jika mana-mana orang boleh dikenakan apa-apa hukuman atau penalti di bawah Akta ini bagi apa-apa perbuatan, peninggalan, pengabaian atau keingkaran yang dilakukan—

- (a) oleh pekerja orang itu dalam perjalanan pekerjaannya;
- (b) oleh ejen orang itu semasa bertindak bagi pihak orang itu; atau
- (c) oleh pekerja ejen orang itu semasa bertindak dalam perjalanan pekerjaannya dengan ejen orang itu atau selainnya bagi pihak ejen orang itu yang bertindak bagi pihak orang itu,

orang itu boleh dikenakan hukuman atau penalti yang sama bagi tiap-tiap perbuatan, peninggalan, pengabaian atau keingkaran oleh pekerja atau ejen orang itu, atau oleh pekerja ejen orang itu.

Pengkompaunan kesalahan

60. (1) Menteri boleh, dengan kelulusan Pendakwa Raya, membuat peraturan-peraturan yang menetapkan—

- (a) apa-apa kesalahan di bawah Akta ini sebagai suatu kesalahan yang boleh dikompaun; dan

(b) kaedah dan tatacara untuk mengkompaun kesalahan itu.

(2) Ketua Eksekutif boleh, dengan keizinan bertulis Pendakwa Raya, mengkompaun apa-apa kesalahan yang dilakukan oleh mana-mana orang di bawah Akta ini yang ditetapkan sebagai suatu kesalahan yang boleh dikompaun dengan membuat suatu tawaran bertulis kepada orang yang disyaki telah melakukan kesalahan itu untuk mengkompaun kesalahan itu apabila dibayar kepada Ketua Eksekutif suatu amaun tidak melebihi lima puluh peratus amaun denda maksimum bagi kesalahan itu dalam masa yang dinyatakan dalam tawaran bertulisnya.

(3) Suatu tawaran di bawah subseksyen (2) boleh dibuat pada bila-bila masa selepas kesalahan itu dilakukan tetapi sebelum apa-apa pendakwaan baginya dimulakan.

(4) Jika amaun yang dinyatakan dalam tawaran itu tidak dibayar dalam masa yang dinyatakan dalam tawaran itu, atau apa-apa lanjutan masa sebagaimana yang diberikan oleh Ketua Eksekutif, pendakwaan bagi kesalahan itu boleh dimulakan pada bila-bila masa selepas itu terhadap orang yang kepadanya tawaran itu dibuat.

(5) Jika suatu kesalahan telah dikompaun di bawah seksyen ini—

(a) tiada pendakwaan boleh dimulakan berkenaan dengan kesalahan itu terhadap orang yang kepadanya tawaran untuk mengkompaun itu dibuat; dan

(b) apa-apa dokumen atau benda yang disita yang berkaitan dengan kesalahan itu boleh dilepaskan oleh Ketua Eksekutif, tertakluk kepada terma sebagaimana yang difikirkan patut oleh Ketua Eksekutif.

(6) Semua jumlah wang yang diterima oleh Ketua Eksekutif di bawah seksyen ini hendaklah dibayar ke dalam dan menjadi sebahagian daripada Kumpulan Wang Disatukan Persekutuan.

Kuasa untuk mengecualikan

61. Menteri boleh, melalui perintah yang disiarkan dalam *Warta*, tertakluk kepada apa-apa syarat atau sekatan yang difikirkannya perlu atau suai manfaat untuk dikenakan, mengecualikan mana-mana orang atau mana-mana golongan orang daripada mana-mana atau semua peruntukan Akta ini.

Kuasa untuk meminda Jadual

62. Menteri boleh, atas syor Ketua Eksekutif, melalui perintah yang disiarkan dalam *Warta*, meminda Jadual kepada Akta ini.

Kuasa untuk membuat peraturan-peraturan

63. (1) Menteri boleh membuat peraturan-peraturan yang perlu atau suai manfaat bagi maksud pelaksanaan peruntukan Akta ini.

(2) Tanpa menjejaskan keluasan subseksyen (1), Menteri boleh membuat peraturan-peraturan untuk menetapkan—

- (a) tempoh bagi membuat penilaian risiko keselamatan siber dan menjalankan audit;
- (b) tempoh dan cara bagaimana maklumat yang berhubungan dengan insiden keselamatan siber hendaklah diberitahu kepada Ketua Eksekutif dan ketua sektor infrastruktur maklumat kritikal negara;
- (c) perkhidmatan keselamatan siber yang berkenaan dengannya suatu lesen hendaklah diperoleh di bawah Akta ini;
- (d) cara bagi permohonan lesen dan pembaharuan lesen di bawah Akta ini;
- (e) fi yang perlu dibayar di bawah Akta ini;
- (f) kesalahan yang boleh dikompaun dan borang yang digunakan dan kaedah dan tatacara untuk mengkompaun kesalahan di bawah Akta ini;
- (g) apa-apa perkara lain yang dikehendaki oleh Akta ini untuk ditetapkan.

(3) Peraturan-peraturan yang dibuat di bawah Akta ini boleh menetapkan suatu perbuatan atau peninggalan yang melanggar peraturan-peraturan itu menjadi suatu kesalahan dan boleh menetapkan penalti denda yang tidak melebihi dua ratus ribu ringgit atau pemenjaraan selama tempoh tidak melebihi tiga tahun atau kedua-duanya.

Kecualian

64. Pada tarikh permulaan kuat kuasa Akta ini, apa-apa langkah, standard dan proses yang telah dilaksanakan untuk memastikan keselamatan siber infrastruktur maklumat kritikal negara dan dikenakan ke atas mana-mana Entiti Kerajaan atau orang di bawah Arahan Majlis Keselamatan Negara No. 26 hendaklah, selagi ia selaras dengan peruntukan Akta ini, terus berkuat kuasa hingga ia dibatalkan di bawah Akta Majlis Keselamatan Negara 2017 [*Akta 776*].

JADUAL

[Seksyen 4]

SEKTOR INFRASTRUKTUR MAKLUMAT KRITIKAL NEGARA

1. Kerajaan
2. Perbankan dan kewangan
3. Pengangkutan
4. Pertahanan dan keselamatan negara
5. Maklumat, komunikasi dan digital
6. Perkhidmatan jagaan kesihatan
7. Air, pembentungan dan pengurusan sisa
8. Tenaga
9. Pertanian dan perladangan
10. Perdagangan, industri dan ekonomi
11. Sains, teknologi dan inovasi

HURAIAN

Rang Undang-Undang ini (“Akta yang dicadangkan”) bertujuan untuk meningkatkan keselamatan siber negara dengan menghendaki pematuhan terhadap langkah-langkah, standard dan proses tertentu dalam pengurusan ancaman keselamatan siber dan insiden keselamatan siber terhadap infrastruktur maklumat kritikal negara. Ini disebabkan oleh penggunaan meluas sistem dan peranti teknologi maklumat dan komunikasi dalam melaksanakan pelbagai fungsi dan urusan sektor awam dan sektor swasta. Bagi maksud ini, Akta yang dicadangkan mengadakan peruntukan, antara lain, bagi penubuhan Jawatankuasa Keselamatan Siber Negara, kewajipan dan kuasa Ketua Eksekutif Agensi Keselamatan Siber Negara, pelantikan ketua sektor infrastruktur maklumat kritikal negara dan penetapan entiti infrastruktur maklumat kritikal negara serta pelesenan pemberi perkhidmatan keselamatan siber.

BAHAGIAN I

2. Bahagian I Akta yang dicadangkan memperkatakan tentang perkara permulaan.
3. *Fasal 1* mengandungi tajuk ringkas Akta yang dicadangkan dan peruntukan mengenai permulaan kuat kuasa Akta yang dicadangkan.
4. *Fasal 2* bertujuan untuk mengadakan peruntukan bahawa Akta yang dicadangkan hendaklah mengikat Kerajaan Persekutuan dan Kerajaan Negeri. Namun, tiada pendakwaan boleh dimulakan terhadap Kerajaan Persekutuan atau mana-mana Kerajaan Negeri bagi apa-apa kesalahan di bawah Akta yang dicadangkan.
5. *Fasal 3* bertujuan untuk mengadakan peruntukan bagi pemakaian luar wilayah Akta yang dicadangkan.
6. *Fasal 4* mengandungi takrif bagi perkataan dan ungkapan tertentu yang digunakan dalam Akta yang dicadangkan.

BAHAGIAN II

7. Bahagian II Akta yang dicadangkan memperkatakan tentang penubuhan Jawatankuasa Keselamatan Siber Negara (“Jawatankuasa”).
8. *Fasal 5* bertujuan untuk mengadakan peruntukan bagi penubuhan dan keanggotaan Jawatankuasa.
9. *Fasal 6* bertujuan untuk mengadakan peruntukan bagi fungsi Jawatankuasa.
10. *Fasal 7* bertujuan untuk mengadakan peruntukan bagi mesyuarat Jawatankuasa. *Fasal* ini juga memperuntukkan bahawa Jawatankuasa boleh menentukan tatacaranya sendiri.
11. *Fasal 8* bertujuan untuk memperuntukkan bahawa Jawatankuasa boleh mengundang mana-mana orang untuk menghadiri mesyuarat Jawatankuasa bagi maksud menasihati Jawatankuasa mengenai apa-apa perkara yang sedang dibincangkan.

12. *Fasal 9* bertujuan untuk memperuntukkan bahawa Jawatankuasa boleh melantik jawatankuasa kecil untuk membantu Jawatankuasa dalam menjalankan fungsinya di bawah Akta yang dicadangkan.

BAHAGIAN III

13. Bahagian III Akta yang dicadangkan memperkatakan tentang kewajipan dan kuasa Ketua Eksekutif Agensi Keselamatan Siber Negara (“Ketua Eksekutif”).

14. *Fasal 10* bertujuan untuk mengadakan peruntukan bagi kewajipan dan kuasa Ketua Eksekutif di bawah Akta yang dicadangkan.

15. *Fasal 11* bertujuan untuk mengadakan peruntukan bagi penubuhan dan penyenggaraan Sistem Pusat Penyelarasan dan Kawalan Siber Negara oleh Ketua Eksekutif bagi maksud menguruskan ancaman keselamatan siber dan insiden keselamatan siber.

16. *Fasal 12* bertujuan untuk memberi Ketua Eksekutif kuasa untuk melantik mana-mana pakar yang berkelayakan dalam keselamatan siber sebagai pakar keselamatan siber dalam perjalanan, atau berkaitan dengan, atau semunasabahnya bersampingan dengan, pelaksanaan kewajipan Ketua Eksekutif di bawah Akta yang dicadangkan. Antara tujuan utama pelantikan seseorang pakar keselamatan siber di bawah Akta yang dicadangkan adalah untuk membantu Ketua Eksekutif dalam menjalankan kewajibannya berhubung dengan insiden keselamatan siber.

17. *Fasal 13* bertujuan untuk memperuntukkan bahawa Ketua Eksekutif boleh mengeluarkan apa-apa arahan bagi maksud memastikan pematuhan Akta yang dicadangkan. Arahan itu hendaklah termasuk antara lain kehendak minimum bagi langkah-langkah, standard dan proses yang berhubung dengan keselamatan siber.

18. *Fasal 14* bertujuan untuk menghendaki mana-mana orang untuk memberi maklumat, butir-butir atau dokumen kepada Ketua Eksekutif jika Ketua Eksekutif mempunyai alasan yang munasabah untuk mempercayai bahawa orang itu mempunyai apa-apa maklumat, butir-butir atau dokumen yang berkaitan dengan pelaksanaan kewajipan dan kuasa Ketua Eksekutif di bawah Akta yang dicadangkan atau bahawa orang itu berupaya untuk memberikan apa-apa keterangan yang Ketua Eksekutif mempunyai alasan yang munasabah untuk mempercayai adalah berkaitan dengan pelaksanaan kewajipan dan kuasa Ketua Eksekutif di bawah Akta yang dicadangkan. Mana-mana orang yang mendedahkan apa-apa maklumat atau mengemukakan apa-apa dokumen di bawah *fasal* ini tidak boleh, semata-mata oleh sebab penzahiran atau pengemukakan itu, didakwa bagi apa-apa kesalahan di bawah mana-mana undang-undang bertulis, atau dikenakan apa-apa prosiding atau tuntutan oleh mana-mana orang di bawah mana-mana undang-undang atau di bawah apa-apa kontrak, perjanjian atau perkiraan, atau selainnya.

BAHAGIAN IV

19. Bahagian IV Akta yang dicadangkan memperkatakan tentang ketua sektor infrastruktur maklumat kritikal negara dan entiti infrastruktur maklumat kritikal negara.

20. *Fasal 15* bertujuan untuk mengadakan peruntukan bagi pelantikan ketua sektor infrastruktur maklumat kritikal negara.

21. *Fasal 16* bertujuan untuk mengadakan peruntukan bagi fungsi ketua sektor infrastruktur maklumat kritikal negara.

22. *Fasal 17* bertujuan untuk mengadakan peruntukan bagi penetapan mana-mana Entiti Kerajaan atau orang sebagai entiti infrastruktur maklumat kritikal negara oleh ketua sektor infrastruktur maklumat kritikal negara jika ketua sektor infrastruktur maklumat kritikal negara itu berpuas hati bahawa entiti infrastruktur maklumat kritikal negara itu memiliki atau mengendalikan suatu infrastruktur maklumat kritikal negara. *Fasal* ini juga mengadakan peruntukan bagi penyimpanan daftar mengenai entiti infrastruktur maklumat kritikal negara yang ditetapkan.

23. *Fasal 18* bertujuan untuk mengadakan peruntukan bagi penetapan ketua sektor infrastruktur maklumat kritikal negara sebagai suatu entiti infrastruktur maklumat kritikal negara oleh Ketua Eksekutif dan penyimpanan daftar bagi penetapan yang dibuat itu oleh Ketua Eksekutif .

24. *Fasal 19* bertujuan untuk mengadakan peruntukan bagi pembatalan penetapan entiti infrastruktur maklumat kritikal negara jika entiti itu tidak lagi memiliki atau mengendalikan apa-apa infrastruktur maklumat kritikal negara.

25. *Fasal 20* bertujuan untuk mengadakan peruntukan bagi kewajipan entiti infrastruktur maklumat kritikal negara untuk memberikan maklumat yang berhubungan dengan infrastruktur maklumat kritikal negaranya kepada ketua sektor infrastruktur maklumat kritikal negara. Entiti infrastruktur maklumat kritikal negara juga dikehendaki untuk memberikan maklumat di bawah *fasal* ini apabila ia memperoleh atau mempunyai dalam milikannya atau kawalannya apa-apa komputer atau sistem komputer tambahan yang pada pendapatnya merupakan infrastruktur maklumat kritikal negara, atau apabila apa-apa perubahan material dibuat terhadap reka bentuk, konfigurasi, keselamatan atau pengendalian infrastruktur maklumat kritikal negaranya yang sedia ada.

26. *Fasal 21* bertujuan untuk mengadakan peruntukan bagi kewajipan entiti infrastruktur maklumat kritikal negara untuk melaksanakan langkah, standard dan proses sebagaimana yang dinyatakan dalam tataamalan atau apa-apa langkah, standard dan proses alternatif atau tambahan bagi maksud memastikan keselamatan siber infrastruktur maklumat kritikal negaranya. Pelaksanaan langkah, standard dan proses di bawah mana-mana undang-undang bertulis yang lain bagi maksud memastikan keselamatan siber infrastruktur maklumat kritikal negara yang tidak bertentangan dengan tataamalan hendaklah disifatkan telah mematuhi *fasal* ini.

27. *Fasal 22* bertujuan untuk mengadakan peruntukan bagi kewajipan entiti infrastruktur maklumat kritikal negara untuk membuat penilaian risiko keselamatan siber dan menyebabkan suatu audit dijalankan dan untuk mengemukakan laporan penilaian risiko keselamatan siber dan laporan audit itu kepada Ketua Eksekutif.

28. *Fasal 23* bertujuan untuk mengadakan peruntukan bagi kewajipan entiti infrastruktur maklumat kritikal negara untuk memberitahu Ketua Eksekutif dan ketua sektor infrastruktur maklumat kritikal negaranya mengenai apa-apa insiden keselamatan siber yang telah atau mungkin telah berlaku berkenaan dengan infrastruktur maklumat kritikal negaranya.

29. *Fasal 24* bertujuan untuk memberi Ketua Eksekutif kuasa untuk menjalankan latihan keselamatan siber bagi maksud menilai kesediaan mana-mana entiti infrastruktur maklumat kritikal negara untuk bertindak balas terhadap mana-mana ancaman keselamatan siber atau insiden keselamatan siber.

BAHAGIAN V

30. Bahagian V Akta yang dicadangkan memperkatakan tentang tataamalan.

31. *Fasal 25* bertujuan untuk mengadakan peruntukan bagi penyediaan dan pengendorsan tataamalan.

32. *Fasal 26* bertujuan untuk menjelaskan bahawa apabila ketua sektor infrastruktur maklumat kritikal negara mengarahkan suatu entiti infrastruktur maklumat kritikal negara untuk melaksanakan langkah, standard dan proses untuk memastikan keselamatan siber infrastruktur maklumat kritikal negaranya di bawah mana-mana undang-undang bertulis yang lain, ketua sektor infrastruktur maklumat kritikal negara itu hendaklah memastikan bahawa arahan yang diberikan adalah selaras dengan tataamalan yang disediakan di bawah *fasal 25*.

BAHAGIAN VI

33. Bahagian VI Akta yang dicadangkan memperkatakan tentang pelesenan pemberi perkhidmatan keselamatan siber.

34. *Fasal 27* bertujuan untuk mengadakan peruntukan bagi pelesenan berhubung dengan pemberi perkhidmatan keselamatan siber. Bagi maksud ini, perkhidmatan keselamatan siber hendaklah sebagaimana yang ditetapkan oleh Menteri.

35. *Fasal 28* bertujuan untuk mengadakan peruntukan bagi kelayakan bagi permohonan lesen di bawah Bahagian ini.

36. *Fasal 29* bertujuan untuk memperuntukkan bahawa permohonan bagi lesen hendaklah dibuat kepada Ketua Eksekutif dan Ketua Eksekutif boleh meluluskan atau menolak permohonan itu.

37. *Fasal 30* bertujuan untuk mengadakan peruntukan bagi pembaharuan lesen.

38. *Fasal 31* bertujuan untuk mengadakan peruntukan bagi kuasa Ketua Eksekutif untuk mengenakan syarat ke atas lesen.

39. *Fasal 32* bertujuan untuk mengadakan peruntukan bagi kewajipan pemegang lesen untuk menyimpan dan menyenggara rekod yang berhubungan dengan perkhidmatan keselamatan siber yang diberikan oleh pemegang lesen.

40. *Fasal 33* bertujuan untuk mengadakan peruntukan bagi pembatalan dan pengantungan lesen.

41. *Fasal 34* bertujuan untuk melarang pemindahmilikan atau penyerahhakan suatu lesen di bawah Akta yang dicadangkan. Walau bagaimanapun, pemindahmilikan lesen itu masih boleh dibuat dengan kelulusan Ketua Eksekutif.

BAHAGIAN VII

42. Bahagian VII of Akta yang dicadangkan memperkatakan tentang insiden keselamatan siber.

43. *Fasal 35* bertujuan untuk mengadakan peruntukan bagi penyiasatan insiden keselamatan siber dan kuasa Ketua Eksekutif untuk mengeluarkan arahan mengenai langkah-langkah yang perlu untuk bertindak balas terhadap atau pulih daripada insiden keselamatan siber itu dan untuk mencegah insiden keselamatan siber itu daripada berlaku pada masa hadapan.

BAHAGIAN VIII

44. Bahagian VIII Akta yang dicadangkan memperkatakan tentang peruntukan penguatkuasaan.

45. *Fasal 36* bertujuan untuk memperuntukkan bahawa Menteri boleh memberikan kuasa kepada mana-mana pegawai awam untuk menjalankan kuasa penguatkuasaan di bawah Akta yang dicadangkan.

46. *Fasal 37* bertujuan untuk mengadakan peruntukan bagi pengeluaran kad kuasa kepada pegawai diberi kuasa.

47. *Fasal 38* bertujuan untuk mengadakan peruntukan bagi kuasa penyiasatan bagi pegawai diberi kuasa.

48. *Fasal 39* memperkatakan tentang peruntukan yang berhubungan dengan pengeledahan dan penyitaan dengan waran.

49. *Fasal 40* memperkatakan tentang peruntukan yang berhubungan dengan pengeledahan dan penyitaan tanpa waran.

50. *Fasal 41* bertujuan untuk menghendaki pegawai diberi kuasa untuk menyediakan senarai barang yang disita dalam perjalanan penyiasatannya.

51. *Fasal 42* bertujuan untuk memperuntukkan bahawa kos memegang mana-mana barang yang disita di bawah Akta yang dicadangkan sementara menunggu penyelesaian prosiding jenayah terhadap seseorang bagi kesalahan di bawah Akta yang dicadangkan hendaklah menjadi hutang yang kena dibayar kepada Kerajaan Persekutuan oleh orang itu dan hendaklah didapatkan kembali apabila orang itu disabitkan.

52. *Fasal 43* bertujuan untuk mengadakan peruntukan bagi pelepasan apa-apa barang yang disita di bawah Akta yang dicadangkan.

53. *Fasal 44* memperkatakan tentang peruntukan yang berhubungan dengan pelucuthakan apa-apa barang yang disita di bawah Akta yang dicadangkan.

54. *Fasal 45* bertujuan untuk memperuntukkan bahawa apa-apa barang yang dilucuthakkan atau disifatkan telah dilucuthakkan di bawah Akta yang dicadangkan hendaklah menjadi harta Kerajaan Persekutuan.

55. *Fasal 46* bertujuan untuk mengadakan peruntukan bagi akses kepada data berkomputer oleh pegawai diberi kuasa. Ini termasuklah akses kepada data berkomputer yang disimpan dalam infrastruktur perkomputeran awan.

56. *Fasal 47* bertujuan untuk memperuntukkan bahawa tiada kos atau ganti rugi yang berbangkit daripada penyitaan mana-mana barang di bawah Akta yang dicadangkan boleh didapatkan dalam mana-mana prosiding di hadapan mana-mana mahkamah melainkan jika penyitaan itu dibuat tanpa sebab yang munasabah.

57. *Fasal 48* bertujuan untuk memperuntukkan bahawa pegawai diberi kuasa boleh menghendaki kehadiran mana-mana orang yang mempunyai pengetahuan tentang fakta dan hal keadaan kes yang sedang disiasat oleh pegawai diberi kuasa.

58. *Fasal 49* bertujuan untuk memperuntukkan bahawa pegawai diberi kuasa boleh memeriksa mana-mana orang yang dikatakan mempunyai pengetahuan tentang fakta dan hal keadaan kes yang sedang disiasat oleh pegawai diberi kuasa.

59. *Fasal 50* bertujuan untuk mengadakan peruntukan bagi kebolehterimaan pernyataan yang dibuat oleh seseorang kepada pegawai diberi kuasa dalam perjalanan suatu penyiasatan yang dibuat di bawah Akta yang dicadangkan sebagai keterangan.

60. *Fasal 51* memperkatakan tentang kuasa tambahan pegawai diberi kuasa bagi maksud pelaksanaan Akta yang dicadangkan.

61. *Fasal 52* bertujuan untuk memperuntukkan bahawa adalah menjadi suatu kesalahan bagi mana-mana orang yang menghalang Ketua Eksekutif atau mana-mana pegawai diberi kuasa dalam pelaksanaan kewajipan mereka di bawah Akta yang dicadangkan.

BAHAGIAN IX

62. Bahagian IX Akta yang dicadangkan memperkatakan tentang peruntukan am.

63. *Fasal 53* bertujuan untuk memperuntukkan bahawa mana-mana orang yang terkilang dengan keengganan Ketua Eksekutif untuk mengeluarkan lesen kepadanya atau dengan pembatalan atau penggantungan lesennya boleh merayu kepada Menteri.

64. *Fasal 54* memperkatakan tentang penyampaian dokumen di bawah Akta yang dicadangkan.

65. *Fasal 55* bertujuan untuk melarang mana-mana anggota Jawatankuasa, Ketua Eksekutif and pegawai diberi kuasa daripada menzahirkan apa-apa maklumat yang diperoleh semasa menjalankan kewajipan mereka melainkan jika penzahiran itu dibuat bagi maksud prosiding undang-undang di bawah mana-mana undang-undang bertulis atau sebagaimana yang diberi kuasa oleh Jawatankuasa.

66. *Fasal 56* bertujuan untuk mengadakan peruntukan bagi perlindungan terhadap Menteri, mana-mana anggota Jawatankuasa, Ketua Eksekutif atau mana-mana pegawai diberi kuasa daripada guaman dan prosiding undang-undang berkenaan dengan apa-apa perbuatan, kecuaiian atau keingkaran yang dilakukan atau ditinggalkan olehnya dalam menjalankan kewajibannya di bawah Akta yang dicadangkan.

67. *Fasal 57* memperuntukkan bahawa tiada pendakwaan boleh dimulakan bagi mana-mana kesalahan di bawah Akta yang dicadangkan tanpa keizinan bertulis Pendakwa Raya.

68. *Fasal 58* memperkatakan tentang tanggungan seorang pengarah, pegawai pematuhan, pekongsi, pengurus, setiausaha atau pegawai lain yang seumpamanya berkenaan dengan kesalahan oleh syarikat, perkongsian liabiliti terhad, firma, pertubuhan atau kumpulan orang yang lain di bawah Akta yang dicadangkan.

69. *Fasal 59* memperkatakan tentang tanggungan seseorang bagi apa-apa perbuatan, peninggalan, pengabaian atau keingkaran yang dilakukan oleh pekerja orang itu, ejen orang itu atau pekerja bagi ejen orang itu di bawah Akta yang dicadangkan.

70. *Fasal 60* bertujuan untuk mengadakan peruntukan bagi pengkompaunan kesalahan di bawah Akta yang dicadangkan.

71. *Fasal 61* bertujuan untuk memberikan kuasa kepada Menteri untuk mengecualikan mana-mana orang atau golongan orang daripada mana-mana atau semua peruntukan Akta yang dicadangkan.

72. *Fasal 62* bertujuan untuk memberikan kuasa kepada Menteri untuk meminda Jadual kepada Akta yang dicadangkan atas syor Ketua Eksekutif.

73. *Fasal 63* bertujuan untuk memberikan kuasa kepada Menteri untuk membuat peraturan-peraturan di bawah Akta yang dicadangkan.

74. *Fasal 64* memperkatakan tentang peruntukan kecualian.

IMPLIKASI KEWANGAN

Rang Undang-Undang ini akan melibatkan Kerajaan dalam perbelanjaan wang tambahan yang amaunnya belum dapat ditentukan sekarang ini.

[PN(U2)3081]