RANCANGAN
UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR ... TAHUN ...
TENTANG
KEAMANAN DAN KETAHANAN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

PRESIDEN REPUBLIK INDONESIA,

Menimbang :

a. bahwa ruang Siber dan ekosistem digital telah menjadi bagian tak terpisahkan dari kehidupan masyarakat dan penyelenggaraan negara serta memiliki pengaruh signifikan terhadap keamanan nasional, stabilitas ekonomi, kehidupan dan kesejahteraan sosial, kedaulatan dan reputasi negara, serta pelayanan publik;
b. bahwa perkembangan teknologi informasi dan komunikasi yang pesat memberi berbagai manfaat untuk kemajuan bangsa dan inovasi di berbagai sektor, teknologi ini juga melahirkan tantangan berupa Ancaman Siber yang menyasar Infrastruktur Informasi, termasuk Infrastruktur Informasi Kritikal;
c. bahwa Ancaman Siber sudah menjadi ancaman paling serius bagi setiap negara termasuk Indonesia, Insiden Siber dapat menyasar Infrastruktur Informasi Kritikal yang berdampak signifikan terhadap pelayanan publik, keamanan dan pertahanan, dan merugikan masyarakat dan negara;
d. bahwa sampai dengan saat ini Indonesia belum memiliki undang-undang Keamanan dan Ketahanan Siber yang sangat diperlukan keberadaannya untuk memberikan kepastian hukum dan menjamin Keamanan dan Ketahanan Siber nasional;
e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c, dan huruf d, perlu membentuk Undang-Undang tentang Keamanan dan Ketahanan Siber;

Mengingat : Pasal 4 ayat (1), Pasal 20, Pasal 21, Pasal 28F, Pasal 28G ayat (1), Pasal 28J, dan Pasal 33 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Dengan Persetujuan Bersama
DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA
dan
PRESIDEN REPUBLIK INDONESIA

MEMUTUSKAN:

Menetapkan : UNDANG-UNDANG TENTANG KEAMANAN DAN KETAHANAN SIBER.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Undang-Undang ini yang dimaksud dengan:

1. Siber adalah segala hal yang berkaitan dengan teknologi informasi, komunikasi elektronik, sistem komputer, dan jaringan yang saling terhubung, mencakup aktivitas virtual seperti pengolahan, penyimpanan, transmisi, dan/atau pertukaran informasi melalui perangkat elektronik dan sistem berbasis komputer.
2. Ruang Siber adalah suatu domain global yang terbentuk dari interkoneksi infrastruktur teknologi informasi termasuk internet, sistem komputer, jaringan komunikasi, dan data.
3. Keamanan Siber adalah pelindungan terhadap Ruang Siber dari berbagai ancaman dan serangan yang dapat merusak dan/atau tindakan yang menyebabkan Infrastruktur Informasi tidak berfungsi, dan/atau gangguan dalam segala bentuknya.
4. Ketahanan Siber adalah kemampuan sistem untuk pulih dan beroperasi kembali secara normal pascainsiden atau setelah mengalami gangguan dan/atau Serangan Siber.
5. Keamanan dan Ketahanan Siber adalah kondisi dinamis Siber yang meliputi seluruh aspek kehidupan nasional yang terintegrasi, aman, dan tangguh serta mampu mengembangkan kekuatan Siber Indonesia dalam menghadapi segala Ancaman Siber terhadap kepentingan Siber Indonesia dan sumber daya yang dikuasai oleh Negara Kesatuan Republik Indonesia.
6. Ancaman Siber adalah segala upaya, kegiatan, dan/atau tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat melemahkan, merugikan, dan/atau menghancurkan kepentingan Siber Indonesia.
7. Serangan Siber adalah tindakan yang dilakukan melalui atau kepada Infrastruktur Informasi yang mengakibatkan rusaknya informasi dan terganggunya atau menjadi tidak berfungsinya Infrastruktur Informasi baik sebagian atau seluruhnya, bersifat sementara atau permanen, secara langsung atau tidak langsung dan/atau merusak sendi-sendi kehidupan bermasyarakat, berbangsa, dan bernegara.

8. Insiden Siber adalah suatu kejadian yang secara aktual atau potensial mengganggu dan/atau merusak informasi dan/atau Infrastruktur Informasi, yang merupakan pelanggaran atau potensi pelanggaran atas kebijakan Keamanan Siber, prosedur keamanan, atau ketentuan penggunaan.
9. Krisis Siber adalah situasi kedaruratan pada media digital akibat dari Insiden Siber pada tingkat nasional atau global yang berdampak terhadap keselamatan, keutuhan, dan kedaulatan negara.
10. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
11. Tata Kelola adalah upaya organisasi dalam menyusun strategi, ekspektasi, dan kebijakan manajemen risiko Keamanan Siber yang meliputi identifikasi, proteksi, deteksi, tanggap, dan pemulihan yang ditetapkan oleh organisasi serta dikomunikasikan dan dipantau implementasinya.
12. Identifikasi adalah proses Keamanan Siber untuk memahami dan mendokumentasikan aset organisasi (data, perangkat keras, perangkat lunak, sistem, fasilitas, dan orang), pemasok, risiko dan ancaman siber yang bertujuan untuk memprioritaskan strategi Keamanan Siber yang berkelanjutan.
13. Proteksi adalah proses Keamanan Siber untuk mendukung kemampuan untuk mengamankan aset guna mencegah atau mengurangi risiko Keamanan Siber yang menimbulkan kerugian.
14. Deteksi adalah proses Keamanan Siber yang bersifat operasional untuk menemukan dan menganalisis secara tepat waktu terhadap anomali yang dapat mengindikasikan terjadinya serangan dan/atau Insiden Siber.
15. Tanggap adalah proses Keamanan Siber untuk menahan dan meminimalisir dampak dari Insiden Siber.
16. Pemulihan adalah proses Keamanan Siber yang bertujuan mengembalikan ke situasi sebagaimana sebelum terjadinya Insiden Siber, dengan membangun komunikasi yang baik selama prosesnya.
17. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
18. Lembaga adalah lembaga eksekutif, legislatif, yudikatif yang menyelenggarakan Infrastruktur Informasi.
19. Infrastruktur Informasi adalah Sistem Elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, yang saling bergantung dengan Sistem Elektronik lainnya.

20. Penyelenggara Infrastruktur Informasi adalah Lembaga, Badan Usaha, dan/atau organisasi Penyelenggara Sistem Elektronik yang memiliki dan/atau mengoperasikan Infrastruktur Informasi.
21. Infrastruktur Informasi Kritikal yang selanjutnya disingkat IIK adalah Infrastruktur Informasi penunjang sektor strategis, yang jika terjadi gangguan, kerusakan, dan/atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.
22. Penyelenggara IIK adalah Penyelenggara Infrastruktur Informasi yang memiliki dan/atau mengoperasikan IIK.
23. Penyedia Produk dan Layanan adalah pihak yang menyediakan perangkat keras, perangkat lunak, sistem, fasilitas, dan/atau orang yang digunakan oleh Penyelenggara Infrastruktur Informasi atau Penyelenggara Sistem Elektronik.
24. Produk dengan Elemen Digital yang selanjutnya disingkat PDED adalah produk perangkat lunak atau perangkat keras beserta layanan pemrosesan data jarak jauh dari produk tersebut, termasuk komponen perangkat lunak atau perangkat keras yang dipasarkan secara terpisah.
25. Pemantauan adalah upaya untuk memahami dinamika dan tren di Ruang Siber dalam rangka merumuskan strategi dan taktik yang efektif dan efisien di lingkup Keamanan dan Ketahanan Siber.
26. Kriptografi merupakan ilmu dan seni menggunakan prinsip, cara, dan metode untuk mengamankan informasi dari akses yang tidak sah dan/atau mengungkap informasi terenkripsi.
27. Badan Siber Republik Indonesia yang selanjutnya disebut Badan yang selanjutnya disebut Badan adalah lembaga yang melaksanakan urusan pemerintah dalam bidang Keamanan dan Ketahanan Siber berdasarkan Undang-Undang ini.
28. Pemerintah Pusat yang selanjutnya disebut Pemerintah adalah Presiden Republik Indonesia yang memegang kekuasaan pemerintahan negara Republik Indonesia yang dibantu oleh Wakil Presiden dan menteri sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
29. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
30. Setiap Orang adalah orang perseorangan termasuk korporasi.

Pasal 2

(1) Undang-Undang ini berlaku bagi Setiap Orang dan/atau Penyelenggara Infrastruktur Informasi yang mengelola

Infrastruktur Informasi atau teknologi informasi dan komunikasi, baik di sektor publik maupun swasta, serta Penyedia Produk dan Layanan Infrastruktur Informasi atau teknologi informasi dan komunikasi lainnya.

(2) Undang-Undang ini berlaku terhadap:
   a. perbuatan hukum yang terjadi di wilayah Indonesia;
   b. perbuatan hukum yang terjadi di atas kapal yang berbendera Indonesia atau pesawat yang terdaftar di bawah hukum Indonesia pada saat perbuatan hukum tersebut dilakukan;
   c. perbuatan hukum dilakukan terhadap warga negara Indonesia;
   d. perbuatan hukum yang dilakukan oleh Setiap Orang Indonesia, asing, atau orang perseorangan yang tanpa kewarganegaraan yang bertempat tinggal tetap di wilayah Indonesia;
   e. pelaksanaan yurisdiksi berdasarkan perjanjian internasional yang telah diratifikasi oleh Indonesia; dan/atau
   f. perbuatan hukum yang dilakukan oleh Setiap Orang Indonesia, asing di luar wilayah Indonesia yang menimbulkan dampak, gangguan, kerugian, dan/atau perbuatan melawan hukum terhadap kedaulatan, keamanan, atau kepentingan Indonesia.

BAB II
ASAS DAN TUJUAN

Pasal 3

Keamanan dan Ketahanan Siber diselenggarakan berasaskan:
a. kedaulatan negara;
b. pelindungan dan kepastian hukum;
c. ekstrateritorialitas;
d. transparansi;
e. inovasi teknologi yang bertanggung jawab;
f. pengembangan ekonomi digital; dan
g. penghargaan dan pelindungan hak asasi manusia.

Pasal 4

Keamanan dan Ketahanan Siber bertujuan:
a. melindungi keutuhan dan kedaulatan Indonesia dari Ancaman Siber baik domestik maupun global;
b. meningkatkan keamanan dan ketahanan sistem informasi dan Infrastruktur Informasi nasional dalam menghadapi Ancaman dan Serangan Siber;
c. mengoptimalkan daya saing dan mendukung inovasi di bidang teknologi digital secara bertanggung jawab dan memenuhi persyaratan Keamanan dan Ketahanan Siber dengan tata kelola yang baik;

d. mengonsolidasikan peran seluruh Lembaga negara dan pemangku kepentingan lainnya yang terlibat dalam penyelenggaraan Keamanan dan Ketahanan Siber secara sinergis dan kolaboratif;
e. mendukung pengembangan ekonomi digital dan memperkuat kerja sama seluruh pemangku kepentingan dalam mendukung pertumbuhan ekonomi dan pemanfaatan Ruang Siber secara tangguh dan aman; dan
f. mendukung kerja sama internasional di bidang Keamanan dan Ketahanan Siber berdasarkan hukum internasional.

BAB III
PENYELENGGARAAN KEAMANAN DAN KETAHANAN SIBER

Bagian Kesatu
Umum

Pasal 5
Dalam menyelenggarakan Keamanan dan Ketahanan Siber, Setiap Orang, Lembaga, dan Penyelenggara Infrastruktur Informasi wajib melindungi Infrastruktur Informasi dan IIK sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 6
Penyelenggaraan Keamanan dan Ketahanan Siber dilakukan melalui:
a. Peran Pemerintah;
b. strategi nasional Keamanan dan Ketahanan Siber ;
c. kerangka kerja Keamanan Siber;
d. tata kelola PDED;
e. kewajiban Penyelenggara IIK, pemantauan, dan evaluasi;
f. pelaporan Insiden Siber; dan
g. koordinasi AntarLembaga.

Bagian Kedua
Peran Pemerintah

Pasal 7
Dalam rangka penyelenggaraan Keamanan dan Ketahanan Siber, Pemerintah melaksanakan:
a. peningkatan kesadaran dan pemahaman serta pembentukan budaya Keamanan dan Ketahanan Siber bagi masyarakat;
b. pemenuhan sertifikasi profesional Keamanan Siber, praktik keamanan Siber, dan pengujian kelemahan sistem, dan bidang tertentu yang ditetapkan oleh Pemerintah;
c. pengembangan dan peningkatan kapasitas sumber daya manusia yang meliputi pendidikan dan pelatihan, peningkatan kompetensi dan bentuk literasi digital lainnya;

d. fasilitasi pengembangan ilmu pengetahuan, teknologi, riset, dan inovasi untuk mendukung Keamanan dan Ketahanan Siber yang berkelanjutan dengan dapat melibatkan pemangku kepentingan dari berbagai sektor;
e. penggunaan teknologi yang memenuhi persyaratan Keamanan dan Ketahanan Siber;
f. pengawasan kepatuhan industri terhadap Undang-Undang ini; dan
g. penindakan terhadap pelanggaran dan kejahatan Siber melalui kerja sama antara Badan, penegak hukum, regulator, dan institusi terkait.

Bagian Ketiga
Strategi Nasional Keamanan dan Ketahanan Siber

Pasal 8

(1) Pemerintah menetapkan strategi nasional Keamanan dan Ketahanan Siber untuk mewujudkan tujuan penyelenggaraan Keamanan dan Ketahanan Siber.
(2) Strategi nasional sebagaimana dimaksud pada ayat (1) disusun oleh Badan dengan melibatkan dan berkoordinasi dengan seluruh kementerian dan/atau Lembaga terkait.
(3) Strategi nasional sebagaimana dimaksud pada ayat (1) dilaksanakan oleh kementerian, Lembaga, industri, dan/atau instansi terkait lainnya.
(4) Pelaksanaan strategi nasional sebagaimana dimaksud dalam ayat (3) dipantau dan dievaluasi oleh Badan dan dilaporkan kepada Presiden.
(5) Ketentuan lebih lanjut terkait strategi nasional Keamanan dan Ketahanan Siber diatur dengan Peraturan Presiden.

Bagian Keempat
Kerangka Kerja Keamanan Siber

Pasal 9

(1) Penyelenggara Infrastruktur Informasi wajib:
    a. mematuhi standar kerangka kerja keamanan siber berdasarkan Undang-Undang ini; dan
    b. menilai dan memperbarui kebijakan keamanan mereka, termasuk keamanan data pelanggan sesuai dengan perubahan ancaman dan kemajuan teknologi secara berkala, dan melibatkan pihak independen untuk menilai efektivitas langkah keamanan yang diambil.
(2) Setiap Penyelenggara IIK wajib menerapkan kerangka kerja Keamanan Siber yang diakui secara internasional atau sesuai dengan standar yang ditetapkan oleh Pemerintah.
(3) Penyedia Produk dan/atau Layanan yang terlibat dalam pengelolaan IIK wajib memastikan bahwa produk dan/atau layanan yang ditawarkan atau dijualnya mematuhi standar

kerangka kerja Keamanan Siber berdasarkan Undang-Undang ini.

(4) Ketentuan lebih lanjut mengenai kerangka kerja dan Standar kerangka kerja Keamanan Siber sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dengan Peraturan Pemerintah.

Bagian Kelima
Tata Kelola PDED

Pasal 10

(1) Kriteria PDED meliputi:
   a. produk kategori standar yang tidak memerlukan sertifikasi atau asesmen;
   b. produk yang memiliki risiko menengah; dan
   c. produk yang memiliki risiko tinggi.

(2) Produk sebagaimana dimaksud pada ayat (1) huruf a, diwajibkan melakukan asesmen mandiri sebelum dipasarkan dan/atau digunakan.

(3) Produk sebagaimana dimaksud pada ayat (1) huruf b dan huruf c, diwajibkan memenuhi syarat lulus asesmen yang dilakukan oleh Badan sebelum dipasarkan dan/atau digunakan.

(4) Dalam melaksanakan ketentuan sebagaimana dimaksud pada ayat (3), Badan dapat bekerja sama dengan lembaga nasional dan internasional.

(5) Pelaksanaan asesmen sebagaimana diatur pada ayat (3) dipungut biaya dan merupakan penerimaan negara bukan pajak Badan.

(6) Ketentuan lebih lanjut terkait penerimaan negara bukan pajak sebagaimana dimaksud pada ayat (5) diatur dengan Peraturan Pemerintah.

(7) Ketentuan lebih lanjut terkait PDED sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) ditetapkan dengan Peraturan Badan.

Pasal 11

(1) Setiap produsen PDED wajib:
   a. mengidentifikasi dan mendokumentasikan keunggulan dan kerentanan serta komponen yang terkandung dalam produk, termasuk menyusun daftar perangkat lunak yang digunakan;
   b. mengatasi dan memulihkan kerentanan, termasuk menyediakan pembaruan keamanan; dan
   c. melaksanakan pengujian dan evaluasi secara berkala terhadap keamanan PDED.

(2) Dalam hal pembaruan keamanan telah tersedia sebagaimana dimaksud pada ayat (1) huruf b, produsen PDED wajib mengungkapkan informasi mengenai kerentanan yang telah diperbaiki, yang paling sedikit

mencakup:
a. deskripsi kerentanan yang diperbaiki;
b. informasi untuk mengidentifikasi PDED yang terdampak;
c. dampak kerentanan dan tingkat keparahannya; dan
d. informasi yang membantu pengguna dalam memperbaiki kerentanan.

(3) Produsen wajib menerapkan kebijakan pengungkapan kerentanan yang terkoordinasi, yang paling sedikit mencakup:
a. fasilitasi pembagian informasi tentang potensi kerentanan dalam PDED, termasuk kerentanan pada komponen pihak ketiga yang terkandung dalam Produk; dan
b. penyediaan alamat kontak bagi pelaporan kerentanan yang ditemukan dalam PDED.

(4) Produsen wajib menyediakan mekanisme yang aman untuk mendistribusikan pembaruan keamanan bagi PDED guna memastikan kerentanan yang dapat dieksploitasi, diperbaiki atau dimitigasi tepat waktu.

(5) Produsen wajib memberitahukan instrumen pembaruan keamanan dan tindakan yang harus dilakukan oleh pengguna.

Pasal 12

(1) PDED sebagaimana dimaksud dalam Pasal 10 ayat (3) wajib memenuhi lulus asesmen dan standar keamanan sesuai dengan kriteria yang ditetapkan dalam Undang-Undang ini.

(2) Lulus asesmen sebagaimana dimaksud pada ayat (1) dibuktikan dengan sertifikat.

(3) Pedoman asesmen dan standar keamanan PDED ditetapkan oleh Badan.

Pasal 13

(1) Kecerdasan artifisial yang dikembangkan, diterapkan, dan/atau dihasilkan oleh produsen PDED wajib memenuhi nilai Etika Kecerdasan Artifisial dengan memperhatikan inklusivitas, kemanusiaan, keamanan, aksesibilitas, transparansi, kredibilitas dan akuntabilitas, pelindungan data pribadi, pembangunan dan lingkungan berkelanjutan, dan pelindungan kekayaan intelektual.

(2) Pengembangan, penerapan, dan/atau produksi kecerdasan artifisial sebagaimana dimaksud pada ayat (1) wajib diberitahukan kepada Badan.

Pasal 14

(1) Produsen wajib menyesuaikan produk PDED sesuai dengan persyaratan yang ditetapkan oleh Pemerintah.

(2) Ketentuan lebih lanjut mengenai persyaratan PDED diatur dengan Peraturan Pemerintah.

Bagian Keenam
Kewajiban Penyelenggara IIK, Pemantauan, dan Evaluasi

Pasal 15

(1) Penyelenggara IIK dan Penyedia Produk dan/atau Layanan yang terkait dengan IIK wajib menggunakan PDED yang memenuhi kriteria dan persyaratan berdasarkan ketentuan Undang-Undang ini.
(2) Penyelenggara IIK dan penyedia layanan Siber IIK menyampaikan laporan evaluasi secara berkala kepada Badan.
(3) Laporan evaluasi sebagaimana dimaksud pada ayat (2) dilakukan secara mandiri.
(4) Penggunaan PDED sebagaimana dimaksud pada ayat (1) dilakukan pemantauan dan evaluasi oleh Badan dalam rangka meningkatkan Keamanan dan Ketahanan Siber nasional.
(5) Hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (4) dapat diumumkan kepada publik untuk meningkatkan transparansi dan akuntabilitas dalam implementasi kebijakan Keamanan Siber, kecuali ketentuan yang diatur dalam Undang-Undang tentang Keterbukaan Informasi Publik.
(6) Berdasarkan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (5), Badan dapat melakukan asesmen dan/atau audit investigatif dalam hal:
    a. Penyelenggara IIK dan penyedia layanan Siber IIK tidak menyampaikan laporan evaluasi sebagaimana dimaksud pada ayat (2); atau
    b. terdapat indikasi pelanggaran.
(7) Ketentuan lebih lanjut mengenai pemantauan, evaluasi, dan pelaporan berkala diatur dengan Peraturan Pemerintah.

Bagian Ketujuh
Pelaporan Insiden Siber

Pasal 16

(1) Pelaporan Insiden Siber dilakukan oleh:
    a. Penyedia Produk dan/atau Layanan;
    b. Penyelenggara Infrastruktur Informasi; dan
    c. Penyelenggara IIK.
(2) Penyedia Produk dan/atau Layanan sebagaimana dimaksud pada ayat (1) huruf a merupakan penyedia layanan teknologi digital atau teknologi sejenis Penyedia Produk dan/atau Layanan yang menjalin kontrak dengan pengguna.
(3) Penyedia Produk dan/atau Layanan sebagaimana dimaksud pada ayat (2) wajib melaporkan kepada

pengguna produk sejak terjadinya Insiden Siber yang melibatkan produknya.

(4) Laporan sebagaimana dimaksud pada ayat (3) memuat paling sedikit layanan perangkat lunak yang diberikan dan melibatkan sistem pendukung dari produk dan/atau layanan perangkat lunak tersebut.

(5) Laporan sebagaimana dimaksud pada ayat (4) disampaikan secara berkala atau sewaktu-waktu apabila diperlukan.

Pasal 17

(1) Setiap Penyelenggara Infrastruktur Informasi sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf b, yang mengalami Insiden Siber wajib segera melaporkan Insiden Siber tersebut kepada Badan dalam waktu tidak lebih dari 3x24 (tiga kali dua puluh empat) jam setelah Insiden Siber terdeteksi, dengan rincian mengenai sifat dan dampak insiden tersebut.

(2) Pelaporan sebagaimana dimaksud dalam Pasal 16 harus mencakup informasi memadai yang memungkinkan Badan melakukan analisis terhadap Insiden Siber, termasuk langkah yang diambil untuk mengatasi insiden serta upaya Pemulihannya.

(3) Badan berhak melakukan penyelidikan atas Penyelenggara Infrastruktur Informasi yang mengalami Insiden Siber untuk mendukung investigasi.

(4) Laporan Insiden Siber yang diberikan digunakan untuk meningkatkan diagnosis pola ancaman dan mengidentifikasi kerentanan, serta mengembangkan kebijakan mitigasi yang lebih efektif.

(5) Laporan sebagaimana dimaksud pada ayat (4) disampaikan secara berkala atau sewaktu-waktu apabila diperlukan.

Pasal 18

(1) Penyelenggara IIK sebagaimana dimaksud dalam Pasal 16 ayat (1) huruf c wajib melaporkan Insiden Siber kepada Badan, dalam waktu 3x24 (tiga kali dua puluh empat) jam terhitung setelah ditemukan adanya Insiden Siber dengan rincian mengenai sifat dan dampak Insiden Siber tersebut.

(2) Penyelenggara IIK wajib melaporkan Insiden Siber kepada Badan, dalam waktu 1x24 (satu kali dua puluh empat) jam terhitung setelah ditemukan adanya Insiden Siber.

(3) Badan sebagaimana dimaksud pada ayat (1) dan ayat (2) menyampaikan informasi kepada Lembaga dan Penyelenggara Infrastruktur Informasi lainnya sebagai upaya pencegahan atau Tanggap Insiden Siber.

(4) Penyelenggara Infrastruktur Informasi termasuk IIK wajib melapor langsung kepada Badan setiap kali terjadi Insiden Siber.

Pasal 19

(1) Berdasarkan analisis terhadap Insiden Siber sebagaimana dimaksud dalam Pasal 18, Badan merekomendasikan:
    a. Insiden Siber yang tidak berpotensi krisis; atau
    b. Insiden Siber berpotensi krisis.
(2) Terhadap Insiden Siber yang tidak berpotensi krisis sebagaimana dimaksud pada ayat (1) huruf a upaya pemulihan dilakukan oleh:
    a. Penyelenggara Infrastruktur Informasi; dan
    b. Penyelenggara IIK.
(3) Upaya pemulihan yang dilakukan oleh Penyelenggara IIK dapat melibatkan Tim Tanggap Insiden Siber sektor dan/atau Tim Tanggap Insiden Siber nasional.
(4) Terhadap Insiden Siber yang berpotensi krisis sebagaimana dimaksud pada ayat (1) huruf b, Badan memberikan rekomendasi penetapan status krisis Siber kepada Presiden.

Pasal 20

(1) Berdasarkan penetapan sebagaimana dimaksud dalam Pasal 19 ayat (4), Presiden membentuk gugus tugas krisis Siber.
(2) Gugus tugas sebagaimana dimaksud pada ayat (2) melapor secara berkala kepada Presiden.
(3) Dalam hal kondisi sudah dapat dikendalikan dan layanan minimum Infrastruktur Informasi telah tersedia dan pulih kembali, gugus tugas mengajukan pengakhiran status Krisis Siber kepada Presiden.

Bagian Kedelapan
Koordinasi AntarLembaga

Pasal 21

(1) Badan membentuk forum koordinasi antarlembaga dan Penyelenggara Infrastruktur Informasi untuk melaksanakan respons yang cepat dan efektif terhadap Ancaman Siber dan/atau Insiden Siber.
(2) Koordinasi antarlembaga mencakup pertukaran informasi, koordinasi langkah mitigasi, serta upaya pengembangan kebijakan Keamanan Siber terintegrasi.
(3) Badan menetapkan prosedur standar koordinasi antarlembaga dan Penyelenggara Infrastruktur Informasi dalam hal Keamanan dan Ketahanan Siber.

BAB IV
PELINDUNGAN SIBER

Bagian Kesatu
Umum

Pasal 22

Pelindungan Siber adalah upaya terpadu untuk melindungi Infrastruktur Informasi, dan IIK yang memanfaatkan teknologi informasi dan/atau layanan digital dari ancaman, dan/atau Insiden Siber, serangan, dan/atau gangguan Siber.

Pasal 23

(1) Penyelenggara Infrastruktur Informasi bertanggung jawab terhadap pelindungan infrastruktur informasi yang dimiliki, dikelola, dimanfaatkan, dan/atau dioperasikannya.
(2) Dalam melaksanakan tanggung jawab sebagaimana dimaksud pada ayat (1), Penyelenggara Infrastruktur Informasi:
    a. menerapkan standar Keamanan Siber;
    b. mengelola risiko; dan
    c. membuat mitigasi risiko.

Pasal 24

Penyelenggara IIK bertanggung jawab:
a. menyusun tata kelola;
b. menerapkan standar keamanan;
c. melakukan audit keamanan;
d. mengelola risiko;
e. melakukan peningkatan kapasitas;
f. melakukan pengukuran tingkat kematangan; dan
g. menggunakan PDED yang telah lulus asesmen dan memenuhi syarat berdasarkan ketentuan peraturan perundang-undangan; dan
h. melakukan pelindungan data dan data pribadi.

Bagian Kedua
Pelindungan Infrastruktur Informasi

Pasal 25

Infrastruktur Informasi meliputi:
a. jaringan internet;
b. pusat data;
c. data elektronik;
d. komputasi awan;
e. sistem elektronik;
f. layanan digital dalam berbagai jenis;
g. infrastruktur telekomunikasi dan penyiaran; dan
h. infrastruktur lain yang digunakan dalam penyelenggaraan Siber.

Pasal 26

(1) Perencanaan, pembangunan, pengoperasian, pemeliharaan, dan pengawasan Infrastruktur Informasi

wajib menerapkan standar Keamanan dan Ketahanan Siber.

(2) Standar Keamanan dan Ketahanan Siber sebagaimana dimaksud pada ayat (1) ditetapkan oleh Badan.

(3) Ketentuan mengenai perencanaan, pembangunan, pengoperasian, pemeliharaan, dan pengawasan Infrastruktur Informasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Pemerintah.

Pasal 27

Pelindungan Infrastruktur Informasi meliputi:

a. identifikasi dan deteksi;
b. proteksi Infrastruktur Informasi;
c. audit keamanan Infrastruktur Informasi;
d. manajemen risiko keamanan Infrastruktur Informasi;
e. asesmen mandiri dan asesmen oleh pihak ketiga independen;
f. penyusunan standar dan kebijakan keamanan siber; dan/atau
g. rencana keberlangsungan bisnis/kegiatan dan rencana pemulihan insiden.

Paragraf 1
Identifikasi dan Deteksi

Pasal 28

Penyelenggara Infrastruktur Informasi harus melakukan identifikasi terhadap sistem elektronik yang dimilikinya.

Pasal 29

(1) Penyelenggara Infrastruktur Informasi melakukan deteksi Keamanan Siber terhadap sistem elektronik yang dimilikinya.

(2) Deteksi Keamanan Siber sebagaimana dimaksud pada ayat (1) dapat dilaksanakan oleh pihak yang ditunjuk oleh Penyelenggara Infrastruktur Informasi dan diberitahukan kepada Badan.

(3) Pihak yang ditunjuk oleh Penyelenggara Infrastruktur Informasi sebagaimana dimaksud pada ayat (2) harus memenuhi kriteria, tata cara, dan persyaratan yang ditetapkan oleh Badan.

(4) Ketentuan lebih lanjut mengenai kriteria, tata cara, dan persyaratan sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Badan

Paragraf 2
Proteksi Infrastruktur Informasi

Pasal 30

(1) Penyelenggara Infrastruktur Informasi harus melakukan proteksi terhadap sistem elektronik yang dimilikinya.
(2) Proteksi sebagaimana dimaksud pada ayat (1) dapat meliputi namun tidak terbatas pada:
    a. proteksi data;
    b. proteksi jaringan; dan
    c. proteksi aplikasi.
(3) Proteksi sebagaimana dimaksud pada ayat (1) dapat dilaksanakan oleh pihak yang ditunjuk oleh Penyelenggara Infrastruktur Informasi dan diberitahukan kepada Badan.
(4) Pihak yang ditunjuk oleh Penyelenggara Infrastruktur Informasi sebagaimana dimaksud pada ayat (2) harus memenuhi kriteria, tata cara, dan persyaratan yang ditetapkan oleh Badan.
(5) Ketentuan lebih lanjut mengenai kriteria, tata cara, dan persyaratan sebagaimana dimaksud pada ayat (3) diatur dengan Peraturan Badan.

Pasal 31

(1) Badan sebagai operabilitas untuk mendorong dan mengembangkan ekosistem dan industri penggunaan kriptografi.
(2) Dalam melaksanakan ketentuan sebagaimana dimaksud pada ayat (1), Badan mendorong persaingan usaha yang sehat dan pengembangan kriptografi.
(3) Dalam hal operabilitas penggunaan kriptografi, Badan berperan sebagai penghubung operabilitas.
(4) Ketentuan sebagaimana dimaksud pada ayat (1) dikecualikan terhadap penggunaan kriptografi di lingkup Pemerintah.
(5) Penggunaan kriptografi di lingkup Pemerintah sebagaimana dimaksud pada ayat (3) dikoordinasikan oleh Badan.
(6) Ketentuan lebih lanjut mengenai peran Badan sebagai penyelenggara penggunaan kriptografi pada lingkup Pemerintah sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah.

Paragraf 3
Audit Keamanan Infrastruktur Informasi

Pasal 32

(1) Penyelenggara Infrastruktur Informasi harus melakukan audit dan manajemen risiko terhadap sistem elektronik yang dimilikinya.
(2) Pelaksanaan audit sebagaimana dimaksud pada ayat (1) dapat dilakukan oleh pihak yang ditunjuk oleh Penyelenggara Infrastruktur Informasi sesuai peraturan perundang-undangan dan diberitahukan kepada Badan.

(3) Untuk melaksanakan ketentuan sebagaimana dimaksud pada ayat (1) dan ayat (2), Badan menetapkan kriteria dan daftar pelaksana audit independen.
(4) Badan menetapkan kriteria Penyelenggara Infrastruktur Informasi yang wajib melakukan audit dan manajemen risiko sebagaimana dimaksud pada ayat (1).
(5) Ketentuan lebih lanjut pelaksanaan audit Keamanan Infrastruktur Informasi, manajemen risiko Keamanan Siber, sertifikasi, dan asesmen PDED diatur dengan Peraturan Badan.

Paragraf 4
Manajemen Risiko Keamanan Infrastruktur Informasi

Pasal 33

(1) Setiap Penyelenggara Infrastruktur Informasi wajib menerapkan manajemen risiko Keamanan Infrastruktur Informasi secara efektif.
(2) Penerapan manajemen risiko Keamanan Infrastruktur Informasi yang efektif sebagaimana dimaksud pada ayat (1) harus memenuhi persyaratan:
    a. kepatuhan terhadap ketentuan peraturan perundang-undangan;
    b. kesesuaian dengan standar keamanan dan ketahanan Siber; dan
    c. sistem pengendalian intern yang berlaku pada Penyelenggara Infrastruktur Informasi.
(3) Penyelenggara Infrastruktur Informasi wajib melaporkan hasil penerapan manajemen risiko Keamanan Infrastruktur Informasi kepada Kementerian atau Lembaga.
(4) Dalam hal Kementerian atau Lembaga sebagai Penyelenggara Infrastruktur Informasi, Kementerian atau Lembaga wajib melaporkan hasil penerapan manajemen risiko Keamanan Siber kepada Badan.
(5) Ketentuan lebih lanjut mengenai penerapan dan pelaporan hasil penerapan manajemen risiko Keamanan Infrastruktur Informasi diatur dengan Peraturan Badan.
(6) Ketentuan mengenai penerapan dan pelaporan hasil penerapan manajemen risiko Keamanan Infrastruktur Informasi di sektor II ditetapkan oleh Kementerian atau Lembaga dengan mengacu pada Peraturan Badan sebagaimana dimaksud pada ayat (5).

Paragraf 5
Asesmen Mandiri dan Asesmen Oleh Pihak Ketiga Independen

Pasal 34

(1) Penyelenggara Infrastruktur Informasi wajib melakukan asesmen mandiri secara berkala untuk memastikan bahwa

sistem dan jaringan yang dikelola memenuhi standar keamanan siber.

(2) Selain asesmen mandiri, Penyelenggara Infrastruktur Informasi wajib untuk melakukan asesmen oleh pihak ketiga independen minimal sekali setiap dua tahun untuk memastikan tingkat keamanan siber yang objektif dan independen.

(3) Asesmen oleh pihak ketiga independen sebagaimana dimaksud pada ayat (2) dilaksanakan oleh lembaga atau badan yang terakreditasi dan terdaftar oleh Pemerintah.

(4) Asesmen mandiri dan asesmen oleh pihak ketiga independen mencakup evaluasi terhadap keamanan jaringan, keamanan data, keamanan aplikasi, kebijakan dan prosedur keamanan yang diterapkan, kemampuan untuk mendeteksi dan merespon Serangan Siber, serta kemampuan dalam penanganan Insiden Siber.

(5) Ketentuan lebih lanjut mengenai asesmen mandiri dan asesmen oleh pihak ketiga independen diatur dengan Peraturan Badan.

Paragraf 6
Penyusunan Standar dan Kebijakan Keamanan Siber

Pasal 35

(1) Badan menetapkan standar nasional dalam Keamanan Siber.

(2) Standar nasional sebagaimana dimaksud pada ayat (1) wajib dilaksanakan oleh penyelenggara atau pemilik Infrastruktur Informasi.

(3) Penyusunan standar Keamanan Siber disusun oleh Badan dan berkoordinasi dengan Kementerian dan/atau Lembaga terkait.

Pasal 36

(1) Badan menyusun panduan bagi penyelenggara dan/atau pemilik Infrastruktur Siber dalam menyusun kebijakan Keamanan Siber di lingkungannya masing-masing.

(2) Setiap Penyelenggara dan/atau pemilik infrastruktur siber menyusun kebijakan Keamanan Siber atas Infrastruktur Siber yang dikelolanya.

(3) Kebijakan sebagaimana dimaksud pada ayat (2) paling sedikit mengatur:
   a. kebijakan penerapan standar Keamanan Siber;
   b. manajemen risiko; dan
   c. tanggap dan mitigasi Insiden Siber.

Bagian Ketiga
Pelindungan Infrastruktur Informasi Kritikal

Pasal 37

(1) Badan menetapkan sektor informasi kritikal dan kriteria IIK yang wajib memenuhi persyaratan Keamanan dan Ketahanan Siber.
(2) Berdasarkan penetapan sektor informasi kritikal sebagaimana dimaksud pada ayat (1), Badan menetapkan IIK.
(3) Badan menetapkan pedoman pengaturan untuk penerapan pelindungan IIK.

Pasal 38

(1) Penyelenggara IIK tertentu wajib melakukan pendaftaran kepada Badan.
(2) Ketentuan mengenai kriteria Penyelenggara IIK yang wajib melakukan pendaftaran diatur dengan Peraturan Presiden.

Pasal 39

(1) Penyelenggara IIK wajib melaksanakan audit Keamanan Siber secara berkala paling sedikit 1 (satu) kali tiap tahun
(2) Audit keamanan siber sebagaimana dimaksud pada ayat (1) dilakukan terhadap komponen yang meliputi paling sedikit:
    a. penerapan kebijakan, standar, dan prosedur Keamanan Siber di lingkungan Penyelenggara IIK.
    b. efektivitas implementasi kontrol Keamanan teknis dan administratif, termasuk pengelolaan risiko Keamanan Siber;
    c. ketaatan terhadap peraturan perundang-undangan dan standar Keamanan Siber yang relevan di sektornya;
    d. pengelolaan insiden Keamanan Siber, termasuk Deteksi, tanggap, dan pemulihan;
    e. pelindungan data dan informasi, termasuk kerahasiaan, keutuhan, otentikasi, nirsangkal, otorisasi, ketersediaan, dan akuntabilitas;
    f. pengelolaan aset teknologi informasi dan komunikasi yang digunakan dalam IIK; dan
    g. pelaporan Insiden Siber.
(3) Penyelenggara IIK sebagaimana dimaksud pada ayat (1) wajib melaporkan hasil audit Keamanan Siber secara berkala kepada Badan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 40

(1) Penyelenggara IIK wajib membuat mitigasi risiko dan rencana Pemulihan pasca Insiden Siber yang komprehensif dan melaksanakan latihan simulasi secara berkala.
(2) Penyelenggara IIK wajib membuat dokumen elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data.

Pasal 41

Pemerintah dapat memberikan penghargaan kepada Penyelenggara IIK yang telah memenuhi standar Keamanan Siber dan memiliki kinerja Keamanan Siber yang baik.

Pasal 42

IIK wajib memenuhi standar Keamanan Siber sesuai dengan pedoman yang ditetapkan oleh Pemerintah.

Pasal 43

(1) Badan melakukan koordinasi, pengawasan, penindakan, dan evaluasi terhadap penggunaan kecerdasan artifisial pada IIK untuk Penyelenggaraan Peningkatan Kapasitas Keamanan Siber.
(2) Ketentuan lebih lanjut terkait koordinasi, pengawasan, penindakan, dan evaluasi terhadap penggunaan kecerdasan artifisial sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Pemerintah.

Pasal 44

(1) Badan melakukan Identifikasi dan penilaian risiko terhadap IIK, yang berpotensi mempengaruhi stabilitas nasional, sosial, ekonomi, pelayanan umum, dan ketertiban umum jika terjadi Insiden Siber.
(2) Setiap Penyelenggara IIK wajib menerapkan langkah pelindungan maksimal, termasuk pembaruan sistem keamanan secara berkala, pemantauan Ancaman Siber, serta penerapan sistem deteksi potensi ancaman secara memadai.
(3) Penyelenggara IIK wajib memiliki rencana Pemulihan komprehensif, yang meliputi langkah untuk meminimalisasi dampak insiden atau gangguan Siber.
(4) Badan dapat mengeluarkan peringatan dini terkait potensi Ancaman Siber.

Bagian Keempat
Pengawasan dan Kepatuhan

Pasal 45

(1) Badan melakukan pengawasan dan Kepatuhan terhadap Penyelenggara Infrastruktur Informasi dalam menerapkan standar Keamanan Siber.
(2) Dalam melakukan pengawasan dan Kepatuhan sebagaimana dimaksud pada ayat (1), Badan memberikan rekomendasi kepada Penyelenggara Infrastruktur Informasi.

Pasal 46

(1) Badan melakukan pengawasan secara teratur terhadap pelaksanaan Keamanan dan Ketahanan Siber oleh

produsen serta Penyelenggara Infrastruktur Informasi yang menyelenggarakan IIK.

(2) Pengawasan sebagaimana dimaksud pada ayat (1) dilakukan terhadap kepatuhan:
   a. pemenuhan persyaratan Keamanan dan Ketahanan Siber;
   b. penyedia PDED untuk memenuhi standar Keamanan Siber yang ditetapkan.

(3) Dalam hal berdasarkan hasil Pengawasan sebagaimana dimaksud pada ayat (1) diketemukan ketidakpatuhan terhadap ketentuan sebagaimana dimaksud pada ayat (2) dikenakan sanksi administratif.

(4) Penyedia PDED yang tidak memenuhi standar Keamanan Siber yang ditetapkan, dilarang menawarkan produk atau layanan digital mereka di pasar nasional.

Bagian Kelima
Tanggung Jawab dan Pelindungan Penyelenggara Infrastruktur Informasi

Pasal 47

(1) Penyelenggara Infrastruktur Informasi bertanggung jawab:
   a. menyusun tata kelola;
   b. menerapkan standar Keamanan;
   c. melakukan audit Keamanan;
   d. mengelola risiko;
   e. melakukan peningkatan kapasitas;
   f. melakukan pengukuran tingkat kematangan; dan
   g. melakukan pelindungan data dan data pribadi.

(2) Pelindungan Infrastruktur Informasi mencakup:
   a. pelindungan terhadap IIK; dan
   b. pelindungan terhadap Infrastruktur Informasi nonkritikal.

Bagian Keenam
Audit dan Penilaian Keamanan dan Ketahanan Siber

Pasal 48

(1) Setiap Penyelenggara IIK wajib menjalani audit Keamanan dan Ketahanan Siber yang dilakukan pihak auditor di bidang Keamanan dan Ketahanan Siber untuk memastikan bahwa kebijakan, prosedur, dan kontrol keamanan yang diterapkan telah memadai.

(2) Hasil audit Keamanan dan Ketahanan Siber wajib diserahkan kepada Badan dalam waktu 30 (tiga puluh) hari setelah audit selesai dan disimpan sebagai bagian dari dokumentasi yang tersedia bagi pihak yang berwenang untuk diperiksa.

(3) Badan menetapkan standar audit Keamanan dan Ketahanan Siber bagi Penyelenggara Infrastruktur

Informasi dan Penyelenggara IIK, serta menyusun pedoman bagi auditor yang terlibat dalam proses ini.

BAB V
KESIAPSIAGAAN DAN KETAHANAN SIBER

Bagian Kesatu
Umum

Pasal 49

Kesiapsiagaan dan Ketahanan Siber meliputi:

a. kepatuhan dan pemenuhan persyaratan atas PDED;
b. identifikasi Ancaman Siber dan kerentanan Siber melalui Pemantauan dan analisis berkelanjutan;
c. deteksi Ancaman Siber secara dini;
d. tanggap Insiden Siber yang cepat dan efektif melalui prosedur penanganan insiden yang telah ditetapkan;
e. manajemen krisis akibat Insiden Siber dengan koordinasi Lembaga dan pihak terkait;
f. tanggap dan pemulihan pasca-Insiden Siber dengan langkah mitigasi dampak dan Pemulihan sistem yang terkena dampak; dan
g. mitigasi risiko Keamanan dan Ketahanan Siber oleh seluruh pengguna PDED dan kementerian dan/atau Lembaga yang ditetapkan oleh Pemerintah.

Pasal 50

(1) Dalam rangka mewujudkan kesiapsiagaan dan Ketahanan Siber sebagaimana dimaksud dalam Pasal 49, Pemerintah dan Penyelenggara Infrastruktur Informasi wajib melakukan segala upaya untuk mencegah terjadinya Insiden Siber.
(2) Dalam meningkatkan kesiapsiagaan dan Ketahanan Siber sebagaimana dimaksud pada ayat (1), Badan berkolaborasi dengan seluruh Lembaga dan pihak untuk melakukan upaya yang terarah dan terencana dalam menghadapi Insiden Siber.
(3) Upaya yang terarah dan terencana sebagaimana dimaksud pada ayat (3) dilakukan dengan namun tidak terbatas pada:
    a. pembentukan Tim Tanggap Insiden Siber;
    b. penanganan Insiden Siber;
    c. manajemen krisis Siber; dan
    d. pembentukan forum analisis dan berbagi informasi Keamanan Siber.

Bagian Kedua
Tim Tanggap Insiden Siber

Pasal 51

(1) Tim Tanggap Insiden Siber dibentuk dalam rangka penanganan Insiden Siber.
(2) Tim Tanggap Insiden Siber terdiri dari:
    a. Tim Tanggap Insiden Siber nasional;
    b. Tim Tanggap Insiden Siber sektoral; dan
    c. Tim Tanggap Insiden Siber organisasi.
(3) Tim Tanggap Insiden Siber nasional sebagaimana dimaksud pada ayat (2) huruf a terdiri dari unsur Badan, kementerian, Lembaga, dan/atau pihak terkait lainnya yang ditetapkan oleh Kepala Badan.
(4) Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud pada ayat (2) huruf b terdiri dari unsur kementerian/lembaga, Penyelenggara IIK, dan Penyelenggara Infrastruktur Informasi yang ditetapkan oleh pejabat kementerian/lembaga sektor.
(5) Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud pada ayat (2) huruf c terdiri dari unsur Penyelenggara IIK dan Penyelenggara Infrastruktur Informasi yang ditetapkan oleh masing-masing pejabatnya.
(6) Tim Tanggap Insiden Siber melapor dan bertanggung jawab kepada kepala Badan.
(7) Ketentuan lebih lanjut mengenai Tim Tanggap Insiden Siber diatur dengan Peraturan Presiden.

Bagian Ketiga
Tanggap Insiden Siber

Pasal 52

(1) Setiap Penyelenggara Infrastruktur Informasi yang mengalami Insiden Siber sebagaimana dimaksud dalam Pasal 19 wajib segera melakukan tindakan Pemulihan, melaporkan kejadian tersebut kepada Badan, dan bekerja sama untuk menyelidiki insiden tersebut.
(2) Badan berkoordinasi dengan Penyelenggara Infrastruktur Informasi dalam menangani Insiden Siber dengan cepat, efektif, dan terukur.
(3) Penyelenggara Infrastruktur Informasi wajib melakukan pencatatan dan perekaman secara rinci seluruh aktivitas Infrastruktur Informasi yang diselenggarakannya.
(4) Pencatatan dan perekaman sebagaimana dimaksud pada ayat (3) wajib disimpan oleh Penyelenggara Infrastruktur Informasi sekurang-kurangnya 3 bulan.

Pasal 53

Kepala Badan mengusulkan penetapan status krisis Siber kepada Presiden.

Pasal 54

Ketentuan lebih lanjut mengenai kesiapsiagaan dan Ketahanan Siber diatur dengan Peraturan Pemerintah.

BAB VI
SUMBER DAYA MANUSIA

Bagian Kesatu
Umum

Pasal 55

(1) Setiap Penyelenggara Infrastruktur Informasi melakukan pembinaan dan pengawasan terhadap sumber daya manusia yang menangani Keamanan dan Ketahanan Siber di organisasinya.
(2) Pembinaan dan pengawasan terhadap sumber daya manusia Keamanan dan Ketahanan Siber sesuai ayat (1) dilakukan sejak proses perekrutan, operasional hingga pemberhentian.
(3) Sumber daya manusia yang bertanggung jawab terhadap Keamanan dan Ketahanan Siber pada Pemerintah Pusat dan Pemerintah Daerah serta Penyelenggara IIK wajib memiliki kompetensi di bidang keamanan siber.
(4) Kompetensi sumber daya manusia Keamanan dan Ketahanan Siber yang dimaksud pada ayat (3) untuk Penyelenggara IIK harus sesuai dengan Standar Kompetensi Kerja Nasional Indonesia bidang Keamanan Siber atau standar kompetensi kerja di bidang keamanan siber yang diakui secara internasional.
(5) Badan mengkoordinasikan pembinaan dan pengawasan sumber daya manusia Keamanan dan Ketahanan Siber pada Pemerintah Pusat dan Pemerintah Daerah serta Penyelenggara IIK.
(6) Ketentuan lebih lanjut mengenai Pembinaan dan Pengawasan sumber daya manusia Keamanan dan Ketahanan Siber diatur dalam Peraturan Pemerintah.

Bagian Kedua
Pengembangan dan Peningkatan Kapasitas
Sumber Daya Manusia Keamanan dan Ketahanan Siber

Pasal 56

(1) Badan mengoordinasikan pelaksanaan pengembangan dan peningkatan kapasitas sumber daya manusia Keamanan dan Ketahanan Siber.
(2) Pengembangan dan peningkatan sumber daya manusia Keamanan dan Ketahanan Siber sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit melalui:
    a. peningkatan kapasitas sumber daya manusia Keamanan dan Ketahanan Siber;

b. pendidikan dan pelatihan sumber daya manusia Keamanan dan Ketahanan Siber.

(3) Ketentuan lebih lanjut mengenai pengembangan dan peningkatan kapasitas sumber daya manusia Keamanan dan Ketahanan Siber diatur dengan Peraturan Pemerintah.

Bagian Ketiga
Peningkatan Kapasitas Sumber Daya Manusia Keamanan dan Ketahanan Siber

Pasal 57

(1) Badan melaksanakan dan/atau mengoordinasikan program peningkatan kapasitas SDM Keamanan dan Ketahanan Siber, termasuk pelatihan, keterampilan kepada pejabat yang terlibat dalam pengelolaan dan pengamanan Infrastruktur Informasi dan sistem teknologi informasi dan komunikasi di sektor publik dan swasta pada umumnya.
(2) Sektor swasta yang mengelola IIK wajib melaksanakan program pelatihan dan simulasi Tangap Insiden Siber, dan pengetahuan mengenai Ancaman Siber.

Bagian Keempat
Pendidikan dan Pelatihan SDM Keamanan dan Ketahanan Siber

Pasal 58

Badan bekerja sama dengan kementerian di bidang pendidikan dan/atau kementerian terkait lainnya untuk melaksanakan peningkatan kesadaran dan literasi Keamanan dan Ketahanan Siber.

Pasal 59

Badan melaksanakan program peningkatan kualitas SDM di bidang Keamanan dan Ketahanan Siber melalui pelatihan Keamanan Siber.

BAB VII
KEAMANAN RANTAI PASOKAN

Bagian Kesatu
Umum

Pasal 60

(1) Penyelenggaraan Keamanan dan Ketahanan Siber memprioritaskan penggunaan produk dan industri jasa dalam negeri, sepanjang tersedia.
(2) Produk dan jasa yang dihasilkan oleh Industri di bidang Keamanan dan Ketahanan Siber harus memenuhi standar sesuai dengan peraturan perundang-undangan.

Bagian Kedua
Pemantauan

Pasal 61

Badan memantau penetapan dan penggunaan teknologi dalam penyelenggaraan Keamanan dan Ketahanan Siber dan tindak lanjut penanganan Insiden Siber oleh Penyelenggara Infrastruktur Informasi.

Bagian Ketiga
Sertifikasi Produk dan Jasa Keamanan Siber

Pasal 62

(1) Setiap produk dan jasa Keamanan Siber yang beredar di Indonesia wajib lulus asesmen dan/atau memiliki sertifikasi dari Lembaga sertifikasi yang diakui oleh Badan.
(2) Sertifikasi sebagaimana dimaksud pada ayat (1) bertujuan untuk memastikan bahwa produk dan jasa tersebut memenuhi standar Keamanan Siber yang berlaku.
(3) Pemerintah mengakui sertifikasi internasional yang setara atau lebih tinggi dengan standar nasional sebagai sertifikasi berdasarkan Undang-Undang ini.
(4) Sertifikasi internasional yang setara atau lebih tinggi dengan standar nasional sebagaimana dimaksud pada ayat (3) ditetapkan oleh Badan.

Bagian Keempat
Panduan Keamanan Rantai Pasokan

Pasal 63

(1) Penyelenggara Infrastruktur Informasi wajib memastikan bahwa perangkat yang digunakan dalam pelaksanaan ~~fungsi~~ fungsi kritikal telah memenuhi standar Keamanan Siber berdasarkan Undang-Undang ini.
(2) Pengembang dan/atau pemasok perangkat yang memasok produk kepada Penyelenggara Infrastruktur Informasi sebagaimana dimaksud pada ayat (1) wajib transparan, menerapkan kontrol keamanan yang memadai, dan memastikan perangkat lunak berfungsi dengan aman.
(3) Penyelenggara Infrastruktur Informasi sebagaimana dimaksud pada ayat (1) wajib melakukan evaluasi dan audit terhadap perangkat lunak penting yang digunakan untuk memastikan kepatuhan terhadap persyaratan keamanan.

Bagian Kelima
Tanggung Jawab Penyedia Produk dan Layanan

Pasal 64

(1) Penyedia Produk dan Layanan yang terkait dengan IIK wajib memastikan bahwa produk dan layanan yang mereka

sediakan memenuhi standar Keamanan Siber yang ditetapkan oleh Pemerintah berdasarkan Undang-Undang ini.

(2) Penyedia Produk dan Layanan Infrastruktur Informasi wajib melakukan penilaian atau mitigasi risiko terhadap potensi kerentanannya serta mengimplementasikan kontrol teknis dan administratif untuk mencegah serangan dan gangguan Siber.

(3) Setiap Penyedia Produk dan Layanan Infrastruktur Informasi wajib melaporkan secara berkala dan segera setiap insiden yang berpotensi membahayakan Keamanan Siber atau Ketahanan sistem yang mereka kelola.

(4) Penyedia Produk dan Layanan Infrastruktur Informasi wajib:
   a. memastikan bahwa produk dan layanan yang mereka sediakan memenuhi standar Keamanan Siber yang ditetapkan oleh Pemerintah berdasarkan Undang-Undang ini;
   b. melakukan penilaian atau mitigasi risiko terhadap potensi kerentanannya serta mengimplementasikan kontrol teknis dan administratif untuk mencegah serangan dan gangguan Siber; dan
   c. melaporkan secara berkala dan segera setiap insiden yang berpotensi membahayakan Keamanan Siber atau Ketahanan sistem yang mereka kelola.

Bagian Keenam
Pengelolaan Risiko Keamanan Siber

Pasal 65

(1) Setiap Penyelenggara IIK wajib melakukan penilaian risiko terhadap Ancaman Siber secara periodik dan mendalam, serta mengambil langkah-langkah mitigasi yang sesuai dengan ketentuan peraturan perundang-undangan.

(2) Setiap Penyelenggara IIK wajib menyusun rencana Pemulihan dan tanggap darurat yang dapat diaktifkan dalam keadaan darurat siber untuk memastikan ketahanan dan keberlanjutan operasional pasca Insiden Siber.

(3) Badan menetapkan pedoman pengelolaan risiko dan Pemulihan, yang wajib dipatuhi oleh Penyelenggara Infrastruktur Informasi.

(4) Setiap Penyelenggara IIK wajib memastikan bahwa personel utama mereka kompeten dalam Keamanan dan Ketahanan Siber.

BAB VIII
KELEMBAGAAN

Bagian Kesatu
Kedudukan

Pasal 66

(1) Dalam melaksanakan tugas negara di bidang Keamanan dan Ketahanan Siber, dibentuk Badan Siber Republik Indonesia.
(2) Badan melaksanakan penyelenggaraan Keamanan dan Ketahanan Siber, berdasarkan Undang-Undang ini.
(3) Dalam melaksanakan tugas sebagaimana dimaksud pada ayat (1), Badan berkoordinasi dengan kementerian dan Lembaga terkait.
(4) Badan adalah Lembaga negara setingkat menteri yang bertanggung jawab langsung kepada Presiden.
(5) Ketentuan lebih lanjut mengenai struktur dan organisasi Badan sebagaimana dimaksud pada ayat (1) diatur dalam Peraturan Presiden.

Bagian Kedua
Tugas, Fungsi, dan Wewenang

Pasal 67

Badan memiliki tugas:
a. merumuskan dan menetapkan kebijakan serta strategi Keamanan dan Ketahanan Siber;
b. menetapkan peraturan pelaksanaan dan/atau pedoman di bidang penyelenggaraan Keamanan dan Ketahanan Siber;
c. melaksanakan pembinaan dan pengawasan Penyelenggara Infrastruktur Informasi;
d. mengidentifikasi, mendeteksi, melindungi, memulihkan, dan mengendalikan kerentanan, serta Tanggap Insiden Siber;
e. melakukan Pemantauan Ancaman Siber dan mengelola pusat manajemen krisis Siber;
f. menyelenggarakan peningkatan kapasitas Keamanan dan Ketahanan Siber nasional;
g. monitoring, evaluasi pelaporan audit dan asesmen IIK;
h. penyelidikan dan analisis Tanggap Serangan Siber; dan
i. melaksanakan asesmen dan standardisasi PDED.

Pasal 68

Badan memiliki fungsi:
a. menyelenggarakan fungsi Keamanan dan Ketahanan Siber;
b. melaksanakan koordinasi Keamanan dan Ketahanan Siber dengan kementerian, Lembaga terkait, dan/atau pemangku kepentingan lainnya;
c. meningkatkan kemampuan sumber daya manusia di bidang Keamanan dan Ketahanan Siber;

d. menyusun strategi, kebijakan, dan regulasi yang mendukung pembangunan ekosistem Keamanan dan Ketahanan Siber;
e. melaksanakan Pendidikan dan pelatihan, termasuk penyelenggaraan Pendidikan tinggi terkait Keamanan dan Ketahanan Siber; dan
f. kolaborasi antara Pemerintah, pelaku usaha, akademisi, dan masyarakat.

Pasal 69

Badan memiliki wewenang:
a. menyusun rencana dan kebijakan nasional di bidang Keamanan dan Ketahanan Siber secara menyeluruh;
b. melaksanakan operasi Keamanan dan Ketahanan Siber;
c. meminta data, informasi, dan laporan terkait penyelenggaraan Keamanan dan Ketahanan Siber, serta potensi dan Insiden Siber dari Penyelenggara IIK;
d. melaksanakan kerja sama dengan Penyelenggara Infrastruktur Informasi;
e. menyusun strategi nasional dan membuat standar Keamanan Siber;
f. penegakan hukum sesuai Undang-Undang ini; dan
g. melakukan penapisan konten yang berpotensi menjadi Ancaman Siber atau telah menjadi Serangan Siber.

Pasal 70

(1) Dalam menyelenggarakan literasi Keamanan Siber, Badan memberdayakan akademisi, pelaku usaha, Penyelenggara Infrastruktur Informasi dan penyelenggara, serta masyarakat.
(2) Badan menyelenggarakan pendidikan tinggi kedinasan dalam rangka meningkatkan kapasitas sumber daya Keamanan dan Ketahanan Siber.
(3) Ketentuan lebih lanjut mengenai pendidikan tinggi kedinasan diatur dalam Peraturan Pemerintah.

Pasal 71

Ketentuan mengenai tata cara pelaksanaan wewenang Badan sebagaimana dimaksud dalam Pasal 70 diatur dalam Peraturan Pemerintah.

Bagian Ketiga
Kerja Sama Penegakan Hukum

Pasal 72

(1) Dalam penegakan hukum, Badan bekerja sama di bidang Keamanan dan Ketahanan Siber dengan aparat penegak hukum.
(2) Dalam melaksanakan penegakan hukum sebagaimana dimaksud pada ayat (1), Badan dapat bekerja sama dengan

Lembaga internasional secara multilateral, regional, dan/atau kerja sama bilateral, dalam menangani kejahatan siber lintas negara.

(3) Penyedia layanan internet dan platform digital yang digunakan untuk kegiatan kejahatan siber wajib bekerja sama dengan penegak hukum dalam pengungkapan identitas pelaku dan menghentikan distribusi Serangan Siber.

(4) Badan berwenang melakukan pencatatan dan perekaman trafik internet dalam rangka melaksanakan penyelenggaraan Keamanan dan Ketahanan Siber.

BAB IX
PEMBIAYAAN

Pasal 73

(1) Pembiayaan untuk penyelenggaraan Keamanan dan Ketahanan Siber bersumber dari:
   a. Anggaran Pendapatan dan Belanja Negara;
   b. Anggaran Pendapat dan Belanja Daerah;
   c. dana pengembangan Keamanan dan Ketahanan Siber nasional;
   d. hibah; dan/atau
   e. sumber pendanaan lain yang sah dan tidak mengikat menurut ketentuan peraturan perundang-undangan.

(2) Hibah sebagaimana dimaksud pada ayat (1) huruf d dapat berupa:
   a. uang;
   b. barang;
   c. fasilitas;
   d. peralatan; dan/atau
   e. jasa.

Pasal 74

(1) Hibah uang sebagaimana dimaksud dalam Pasal 73 ayat (2) huruf a dimaksudkan dalam dana pengembangan Keamanan dan Ketahanan Siber nasional dan dikelola oleh Badan.

(2) Hasil pengelolaan dana pengembangan Keamanan dan Ketahanan Siber nasional sebagaimana dimaksud pada ayat (1) digunakan untuk:
   a. pengembangan sumber daya manusia;
   b. penelitian;
   c. pemberian penghargaan; dan/atau
   d. dana cadangan untuk mengantisipasi keperluan kontijensi atas terjadinya Insiden Siber dan/atau Serangan Siber.

(3) Ketentuan lebih lanjut tentang pengelolaan dana pengembangan Keamanan dan Ketahanan Siber nasional sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dalam Peraturan Badan.

Pasal 75

(1) Hibah barang, fasilitas, peralatan, dan/atau jasa sebagaimana dimaksud dalam Pasal 76 ayat (2) huruf b, huruf c, huruf d, dan huruf e dikelola oleh Badan.
(2) Pengelolaan hibah barang, fasilitas, peralatan, dan/atau jasa sebagaimana dimaksud pada ayat (1) digunakan untuk peningkatan kemampuan penyelenggaraan Keamanan dan Ketahanan Siber nasional.
(3) Ketentuan lebih lanjut tentang pengelolaan hibah barang, fasilitas, peralatan, dan/atau jasa sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dalam Peraturan Badan.

Pasal 76

(1) Pemerintah Pusat dan Pemerintah Daerah wajib mengalokasikan dana penyelenggaraan Keamanan dan Ketahanan Siber dalam anggaran pendapatan dan belanja negara dan anggaran pendapatan dan belanja daerah.
(2) Dana penyelenggaraan Keamanan dan Ketahanan Siber sebagaimana dimaksud pada ayat (1) diperuntukan untuk:
    a. pengembangan sumber daya manusia; dan
    b. pembangunan dan/atau penguatan perangkat dan infrastruktur Keamanan dan Ketahanan Siber.
(3) Ketentuan lebih lanjut mengenai pengalokasian dan peruntukan dana penyelenggaraan Keamanan dan Ketahanan Siber sebagaimana dimaksud pada ayat (1) dan ayat (2) diatur dalam Peraturan Pemerintah.

BAB IX
KERJA SAMA INTERNASIONAL

Pasal 77

(1) Badan menjalin kerja sama internasional yang berkaitan dengan Keamanan dan Ketahanan Siber .
(2) Kerja sama internasional juga mencakup upaya bersama untuk menangani Ancaman Siber yang bersifat transnasional dan merespons serangan yang dapat mempengaruhi negara lain.
(3) Kerja sama dilakukan berdasarkan perjanjian internasional yang telah diratifikasi oleh Indonesia, kesepakatan multilateral, regional, dan/atau bilateral.

Pasal 78

(1) Dalam rangka memajukan kepentingan Siber Indonesia di tingkat internasional dan turut dalam Keamanan dan Ketahanan Siber global, Badan berpartisipasi dalam berbagai program dan kegiatan global.
(2) Dalam melaksanakan ketentuan sebagaimana dimaksud pada ayat (1), Pemerintah:
    a. berpartisipasi dalam menciptakan, merumuskan, memajukan usulan atau inisiatif konsep, norma, perilaku, dan panduan internasional dalam Keamanan

dan Ketahanan Siber secara bilateral, regional atau multilateral;

b. berpartisipasi dalam kegiatan pemecahan masalah Keamanan dan Ketahanan Siber di forum bilateral, regional atau multilateral;

c. berpartisipasi dalam pengadministrasian rezim internasional di bidang Keamanan dan Ketahanan Siber di tingkat regional atau multilateral;

d. menjalin kemitraan, kerja sama, dan hubungan timbal balik dengan berbagai negara dan/atau Penyelenggara Infrastruktur Informasi internasional untuk meningkatkan Keamanan dan Ketahanan Siber;

e. menyelenggarakan pertemuan baik bilateral maupun multilateral tentang Keamanan dan Ketahanan Siber; dan

f. upaya lain sesuai dengan ketentuan peraturan perundang-undangan dan/atau hukum internasional.

Pasal 79

(1) Badan bekerja sama dan berkoordinasi dengan kementerian dan/atau Lembaga terkait yang bertanggung jawab dalam urusan luar negeri untuk melaksanakan diplomasi Siber.

(2) Kementerian yang bertanggung jawab dalam urusan luar negeri, dalam rangka mengefektifkan pelaksanaan diplomasi Siber sebagaimana dimaksud pada ayat (1), dapat menetapkan atase Keamanan dan Ketahanan Siber.

BAB X
PARTISIPASI MASYARAKAT

Pasal 80

(1) Masyarakat dapat berpartisipasi secara langsung maupun tidak langsung dalam mendukung terselenggaranya Keamanan dan Ketahanan Siber.

(2) Ketentuan mengenai bentuk partisipasi masyarakat ditetapkan dalam Peraturan Badan.

BAB XI
PENYIDIKAN

Pasal 81

Penyidikan terhadap tindak pidana sebagaimana dimaksud dalam Undang-Undang ini, dilakukan berdasarkan ketentuan dalam Hukum Acara Pidana dan ketentuan dalam Undang-Undang ini.

Pasal 82

(1) Selain Penyidik Pejabat Polisi Negara Republik Indonesia, Pejabat Pegawai Negeri Sipil tertentu di lingkungan

Pemerintah yang lingkup tugas dan tanggung jawabnya di bidang Keamanan dan Ketahanan Siber diberi wewenang khusus sebagai penyidik sebagaimana dimaksud dalam undang-undang tentang hukum acara pidana untuk melakukan penyidikan tindak pidana di bidang Keamanan dan Ketahanan Siber.

(2) Penyidikan tindak pidana di bidang Keamanan dan Ketahanan Siber sebagaimana dimaksud pada ayat (1) dilakukan dengan memperhatikan pelindungan terhadap privasi, kerahasiaan, kelancaran layanan publik, dan integritas atau keutuhan data sesuai dengan ketentuan peraturan perundang-undangan.

(3) Penggeledahan dan/atau penyitaan terhadap Sistem Elektronik yang terkait dengan dugaan tindak pidana di bidang Keamanan dan Ketahanan Siber dilakukan sesuai dengan ketentuan hukum acara pidana.

(4) Dalam melakukan penggeledahan dan/atau penyitaan sebagaimana dimaksud pada ayat (3), penyidik wajib menjaga terpeliharanya kepentingan pelayanan umum.

(5) Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) berwenang:

a. menerima laporan atau pengaduan dari seseorang tentang adanya tindak pidana di bidang Keamanan dan Ketahanan Siber;
b. memanggil Setiap Orang atau pihak lainnya untuk didengar dan diperiksa sebagai tersangka atau saksi sehubungan dengan adanya dugaan tindak pidana di bidang Keamanan dan Ketahanan Siber;
c. melakukan pemeriksaan atas kebenaran laporan atau keterangan berkenaan dengan tindak pidana di bidang Keamanan dan Ketahanan Siber;
d. melakukan pemeriksaan terhadap Setiap Orang yang patut diduga melakukan tindak pidana di bidang Keamanan dan Ketahanan Siber;
e. melakukan pemeriksaan terhadap alat dan/atau sarana yang berkaitan dengan kegiatan teknologi informasi yang diduga digunakan untuk melakukan tindak pidana di bidang Keamanan dan Ketahanan Siber;
f. melakukan penggeledahan terhadap tempat tertentu dan/atau Sistem Elektronik yang diduga digunakan sebagai tempat untuk melakukan tindak pidana di bidang Keamanan dan Ketahanan Siber;
g. melakukan penyegelan dan penyitaan terhadap alat dan/atau sarana kegiatan teknologi informasi yang diduga digunakan secara menyimpang dari ketentuan peraturan perundang-undangan;
h. membuat suatu data dan/atau Sistem Elektronik yang terkait tindak pidana di bidang Keamanan dan Ketahanan Siber agar tidak dapat diakses;

i. meminta informasi yang terdapat di dalam Sistem Elektronik atau informasi yang dihasilkan oleh Sistem Elektronik kepada Penyelenggara Infrastruktur Informasi yang terkait dengan tindak pidana di bidang Keamanan dan Ketahanan Siber;
j. meminta bantuan ahli yang diperlukan dalam penyidikan terhadap tindak pidana di bidang Keamanan dan Ketahanan Siber;
k. mengadakan penghentian penyidikan tindak pidana di bidang Keamanan dan Ketahanan Siber sesuai dengan ketentuan hukum acara pidana; dan/atau
l. memerintahkan kepada Penyelenggara Infrastruktur Informasi untuk melakukan pemutusan Akses secara sementara terhadap akun media sosial, rekening bank, uang elektronik, dan/atau aset digital.

(6) Penangkapan dan penahanan terhadap pelaku tindak pidana di bidang Keamanan dan Ketahanan Siber dilakukan sesuai dengan ketentuan hukum acara pidana.
(7) Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) dalam melaksanakan tugasnya memberitahukan dimulainya penyidikan kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.
(8) Dalam hal penyidikan sudah selesai, Penyidik Pejabat Pegawai Negeri Sipil sebagaimana dimaksud pada ayat (1) menyampaikan hasil penyidikannya kepada Penuntut Umum melalui Penyidik Pejabat Polisi Negara Republik Indonesia.
(9) Dalam rangka mengungkap tindak pidana di bidang Keamanan dan Ketahanan Siber, penyidik dapat bekerja sama dengan penyidik negara lain untuk berbagi informasi dan alat bukti sesuai dengan ketentuan peraturan perundang-undangan.

BAB XII
KEWAJIBAN DAN SANKSI ADMINISTRATIF

Bagian Kesatu
Kewajiban

Pasal 83

Setiap Penyelenggara Infrastruktur Informasi wajib:
a. memenuhi standar Keamanan dan Ketahanan Siber yang telah ditetapkan oleh Pemerintah;
b. melaporkan insiden Siber IIK kepada Badan dalam waktu yang telah ditetapkan;
c. memenuhi ketentuan terkait pelindungan data pribadi sesuai dengan peraturan perundang-undangan;
d. menyusun dan menerapkan rencana kesiapsiagaan dan Ketahanan Siber yang memadai;

e. melakukan uji penetrasi dan audit Keamanan Siber secara berkala terhadap sistem dan jaringan Siber; dan
f. menyediakan laporan tahunan terkait upaya dan langkah-langkah yang telah diambil untuk memastikan Keamanan dan Ketahanan Siber dan melaporkannya kepada Badan.

Bagian Kedua
Sanksi Administratif

Pasal 84

(1) Pelanggaran terhadap ketentuan Pasal 10 ayat (2), Pasal 10 ayat (3), Pasal 13, Pasal 16 ayat (3), Pasal 17 ayat (1), Pasal 18 ayat (1), Pasal 18 ayat (2), Pasal 18 ayat (4), Pasal 26 ayat (1), Pasal 34 ayat (4), Pasal 35 ayat (1), Pasal 35 ayat (3), Pasal 35 ayat (4), Pasal 36 ayat (2), Pasal 38 ayat (1), Pasal 39, Pasal 40 ayat (1), Pasal 40 ayat (3), Pasal 41, Pasal 43, Pasal 45 ayat (2), Pasal 45 ayat (3), Pasal 49 ayat (1), Pasal 49 ayat (2), Pasal 51 ayat (1), Pasal 53 ayat (1), Pasal 53 ayat (3), Pasal 53 ayat (4), Pasal 56 ayat (3), Pasal 56 ayat (4), Pasal 58 ayat (2), Pasal 63 ayat (1), Pasal 64, Pasal 65, Pasal 66, Pasal 74 ayat (3), Pasal 78 ayat (1), dan Pasal 85.
(2) Sanksi administratif sebagaimana dimaksud pada ayat (1) berupa:
    a. peringatan tertulis;
    b. penghentian sementara kegiatan usaha;
    c. penghentian permanen atau pembekuan kegiatan usaha; dan/atau
    d. denda administratif.
(3) Pelanggaran terhadap ketentuan Pasal 9 ayat (1), Pasal 9 ayat (2), Pasal 9 ayat (3), Pasal 11, Pasal 12 ayat (1), Pasal 14 ayat (1), Pasal 15 ayat (1) dikenai sanksi administratif berupa denda administratif paling tinggi 2 (dua) persen dari pendapatan kotor tahunan atau penerimaan kotor tahunan terhadap variabel pelanggaran.
(4) Penjatuhan sanksi administratif sebagaimana dimaksud pada ayat (2) diberikan oleh Badan.
(5) Ketentuan lebih lanjut mengenai tata cara pengenaan sanksi administratif sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Pemerintah.

BAB XIII
KETENTUAN PIDANA

Pasal 85

Setiap Orang yang dengan sengaja dan melawan hukum melakukan tindakan apa pun yang mengganggu, merusak, atau melumpuhkan Sistem Elektronik, jaringan elektronik, atau sumber daya elektronik yang merupakan bagian dari IIK, atau mengakibatkan terganggunya IIK dan/atau IIK tidak berfungsi

sebagaimana mestinya, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan/atau denda paling banyak Rp15.000.000.000,00 (lima belas miliar rupiah).

Pasal 86

Setiap Orang yang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, mendistribusikan, atau menyediakan perangkat yang dirancang atau dikembangkan secara khusus untuk memfasilitasi tindakan apa pun yang mengganggu, merusak, atau melumpuhkan Sistem Elektronik, jaringan elektronik, atau sumber daya elektronik yang merupakan bagian dari IIK atau mengakibatkan terganggunya IIK dan/atau IIK tidak berfungsi sebagaimana mestinya, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun serta dan/atau paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 87

Setiap Orang yang dengan sengaja dan melawan hukum dengan cara apapun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan Informasi Elektronik dan/atau dokumen elektronik yang merupakan bagian dari IIK atau yang mengakibatkan Informasi Elektronik dan/atau dokumen elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).

Pasal 88

Setiap Orang yang dengan sengaja dan melawan hukum melakukan serangan dan/atau peretasan Siber dengan maksud membuat kerusakan, gangguan, atau penghentian layanan IIK, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan/atau denda paling banyak Rp15.000.000.000,00 (lima belas miliar rupiah).

Pasal 89

(1) Setiap Orang yang dengan sengaja melakukan peretasan yang mengakibatkan terganggunya Sistem Elektronik atau membuat data tidak dapat diakses oleh pihak yang berhak, dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000 (dua miliar rupiah).
(2) Dalam hal tindak pidana sebagaimana dimaksud pada ayat (1) disertai dengan meminta tebusan atau dilakukan dengan perangkat lunak pemerasan, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan/atau denda paling banyak Rp15.000.000.000 (lima belas miliar rupiah).

(3) Dalam hal tindak pidana sebagaimana dimaksud pada ayat (1) atau ayat (2) dilakukan pada IIK, dipidana dengan pidana pokok ditambah 1/3 (sepertiga).

Pasal 90

Setiap Orang yang dengan sengaja mengakses, mengambil, data IIK dari Sistem Elektronik secara tanpa hak dan di luar kewenangannya, dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp7.000.000.000 (tujuh miliar rupiah).

Pasal 91

Setiap Orang yang dengan sengaja mengubah, memanipulasi, atau merusak data dalam Sistem Elektronik yang mengakibatkan kerugian finansial atau non-finansial, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp6.000.000.000 (enam miliar rupiah).

Pasal 92

Setiap Orang yang dengan sengaja mengendalikan, mengoperasikan, atau menggunakan jaringan perangkat yang terinfeksi (*botnet*) untuk tujuan ilegal dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp9.000.000.000 (sembilan miliar rupiah).

Pasal 93

Setiap Orang yang dengan sengaja mengintimidasi, memengaruhi, atau mengganggu proses penegakan hukum dalam tindak pidana Siber, dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp.5.000.000.000 (lima miliar rupiah).

Pasal 94

Setiap Orang yang dengan sengaja melakukan pencurian atau pengumpulan informasi rahasia milik negara atau yang memiliki nilai strategis nasional melalui sarana Siber, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah).

Pasal 95

Setiap Orang yang dengan sengaja menggunakan sarana Siber untuk melakukan tindak pidana terorisme sebagaimana dimaksud dalam peraturan perundang-undangan di bidang pemberantasan tindak pidana terorisme, dipidana dengan pidana penjara paling lama 20 (dua puluh) tahun, pidana penjara seumur hidup atau pidana mati.

Pasal 96

Setiap Orang yang melakukan Serangan Siber terhadap sistem atau jaringan komputer negara lain yang mengakibatkan kerusakan, gangguan, atau kegagalan fungsi sistem pertahanan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun.

Pasal 97

Setiap Orang yang dengan sengaja membuat, menyebarluaskan, atau memfasilitasi penyebaran konten *deepfake* yang mengakibatkan kekacauan publik, merugikan kepentingan nasional dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).

Pasal 98

Setiap Orang yang dengan sengaja membuat, menyebarluaskan, atau memfasilitasi penyebaran konten *deepfake* yang menyerang kehormatan orang lain, dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

Pasal 99

Setiap Orang yang dengan sengaja melakukan penampungan atau penyaluran dana, termasuk mata uang kripto hasil kejahatan Siber, dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah).

BAB XIV
KETENTUAN PERALIHAN

Pasal 100

Pada saat Undang-Undang ini mulai berlaku, semua peraturan perundang-undangan yang mengatur mengenai Keamanan dan Ketahanan Siber dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan ketentuan dalam Undang-Undang ini.

Pasal 101

Organisasi atau badan yang merupakan unsur penyelenggaraan Keamanan dan Ketahanan Siber yang sudah ada tetap berlaku sampai dengan diubah atau diganti dengan organisasi atau badan baru berdasarkan ketentuan dalam Undang-Undang ini..

Pasal 102

Penyelenggara IIK, Lembaga, dan Penyelenggara Infrastruktur Informasi wajib menyesuaikan dengan Undang-Undang ini, paling lama 2 (dua) tahun sejak Undang-Undang ini diundangkan.

BAB XV
KETENTUAN PENUTUP

Pasal 103

Peraturan pelaksanaan Undang-Undang ini harus telah ditetapkan paling lama 2 (dua) tahun terhitung sejak Undang-Undang ini diundangkan.

Pasal 104

Undang-Undang ini mulai berlaku pada tanggal diundangkan.

Agar Setiap Orang mengetahuinya, memerintahkan pengundangan Undang-Undang ini dengan penempatannya dalam Lembaran Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal ...

PRESIDEN REPUBLIK INDONESIA,

PRABOWO SUBIANTO

Diundangkan di Jakarta
pada tanggal ...

MENTERI SEKRETARIS NEGARA
REPUBLIK INDONESIA

PRASETYO HADI

LEMBARAN NEGARA REPUBLIK INDONESIA TAHUN ... NOMOR ...

PENJELASAN
ATAS
RANCANGAN UNDANG-UNDANG REPUBLIK INDONESIA
NOMOR ... TAHUN ...
TENTANG
KEAMANAN DAN KETAHANAN SIBER

I. UMUM

Ruang Siber dan ekosistem digital telah menjadi bagian tak terpisahkan dari kehidupan masyarakat dan penyelenggaraan negara serta memiliki pengaruh signifikan terhadap Keamanan nasional, stabilitas ekonomi, kesejahteraan sosial, reputasi negara, dan pelayanan publik. Transformasi digital selain memberikan manfaat besar bagi kehidupan manusia juga telah menimbulkan berbagai potensi disrupsi dan gangguan keamanan dan Ketahanan Siber . Dunia siber yang terus berkembang telah menciptakan tantangan baru dalam menjaga keamanan dan kedaulatan nasional, serta memelihara stabilitas ekonomi, pelayanan publik, dan kesejahteraan sosial.

Secara filosofis, pengaturan terkait Keamanan dan Ketahanan/ Siber menggunakan berbagai pendekatan yang saat ini diterapkan dunia internasional dan berbagai negara dalam bentuk pendekatan *cybersecurity* dan *cyberresilience*. Hal ini mencerminkan pengakuan serta pelindungan kepentingan umum serta pelindungan terhadap hak-hak dasar manusia untuk memperoleh kehidupan yang aman dan dilindungi oleh negara. Dengan demikian, penyusunan Undang-Undang tentang Keamanan dan Ketahanan Siber (UU KKS) memiliki dasar filosofis yang kokoh dan dapat dipertanggungjawabkan.

Pancasila dalam hal ini menjadi landasan filosofi utama dalam kaitannya dengan jaminan keamanan dan Ketahanan Siber . Pancasila sebagai *rechtsidee* (cita hukum) yang merupakan konstruksi berpikir dalam mengarahkan hukum kepada apa yang menjadi cita-cita bangsa. Selain dengan dasar filosofis, penyusunan UU KKS pun menggunakan pendekatan sosiologis, yuridis, dan pendekatan hukum transformatif.

Untuk menghadapi ancaman dan kejahatan siber, diperlukan legislasi dengan pendekatan komprehensif transformatif sebagai dasar penyelenggaraan Keamanan dan Ketahanan Siber nasional. Keamanan Siber adalah pelindungan terhadap Ruang Siber dari berbagai ancaman dan serangan yang dapat merusak integritas, kerahasiaan, ketersediaan informasi, atau tindakan yang menyebabkan infrastruktur informasi tidak berfungsi, atau gangguan dalam segala bentuknya. Sedangkan ketahanan dalam UU ini dimaksudkan sebagai Siber adalah kemampuan sistem untuk pulih dan beroperasi kembali secara normal pasca insiden atau setelah mengalami gangguan dan/atau Serangan Siber.

Hukum pada hakikatnya terdiri dari unsur asas, kaidah, lembaga, dan proses-proses. UU KKS harus ditetapkan berdasarkan landasan asas dan filosofi negara, yang dituangkan ke dalam kaidah atau norma. Di samping itu, diperlukan keberadaan lembaga yang kuat yang bisa menghadapi berbagai tantangan keamanan dan Ketahanan Siber serta proses-proses kolaboratif yang dilakukan antarlembaga untuk sepenuhnya menjaga kepentingan nasional. Dengan demikian, keberadaan Badan Siber dan Sandi Negara

(BSSN) perlu ditingkatkan statusnya menjadi lembaga yang lahir dari undang-undang dan setara dengan kementerian yang dapat mengolaborasikan dan mengoordinasikan keamanan dan Ketahanan Siber nasional.

Regulasi mengenai Keamanan dan Ketahanan Siber telah diatur di berbagai negara dan menjadi bagian dari hukum internasional. Regulasi-regulasi dimaksud dapat dijadikan rujukan komparatif dalam penyusunan regulasi keamanan dan Ketahanan Siber nasional Indonesia. UU KKS perlu menekankan pentingnya strategi nasional dan pembagian tanggung jawab antarlembaga yang jelas dalam menghadapi ancaman siber. RUU ini diproyeksikan untuk melindungi Infrastruktur Informasi khususnya Infrastruktur Informasi Kritikal (IIK).

UU KKS disusun sebagai respon dalam menghadapi ancaman siber, menciptakan ekosistem siber yang aman, resilien, dan tangguh dengan tetap mendorong pemanfaatan, pertumbuhan, dan inovasi teknologi. Pelindungan Keamanan dan Ketahanan Siber merupakan suatu bentuk kehadiran negara. Semua elemen dan pemangku kepentingan termasuk penyedia Produk dengan Elemen Digital (PDED) harus berkolaborasi dalam mendukung keamanan dan Ketahanan Siber .

IIK yang berfungsi dalam pelayanan kritikal bagi masyarakat dan kepentingan umum kerap menjadi target utama ancaman siber yang dapat menyebabkan kerugian dan kerentanan keamanan. Oleh karena itu, diperlukan kerangka hukum dan kebijakan yang kuat untuk menjaga Keamanan dan Ketahanan Siber secara holistik, terintegrasi, tanpa ego sektoral, dan komprehensif sehingga kepentingan publik dapat dilindungi dalam situasi apapun.

UU KKS diproyeksikan untuk diterapkan dalam kerangka keamanan dan Ketahanan Siber sejak level hulu atau level awal, dalam arti UU KKS memberikan persyaratan terpenuhinya kriteria keamanan dan ketahanan produk dengan elemen digital sebelum dipasarkan dan digunakan oleh pengguna Infrastruktur Digital atau Infrastruktur Informasi. Pendekatan ini dikombinasikan dengan pendekatan pada level tengah atau pada saat seluruh kegiatan dilakukan beserta prosesnya. Di level ini, UU KKS mengharuskan adanya monitoring, evaluasi, dan asesmen. Pendekatan selanjutnya adalah di level hilir dalam arti UU ini akan memberikan sanksi terhadap segala pelanggaran atas tidak terpenuhinya kewajiban-kewajiban yang diamanatkan pada level hulu dan level menengah. Dengan pendekatan ini, maka UU KKS menjadi kerangka keamanan dan Ketahanan Siber dari mulai level hulu, level menengah (proses monitoring dan evaluasi), dan di level hilir (*downstream regulation*) dalam bentuk kuratif *ultimum remedium* sebagai reaksi terhadap pelanggaran dan insiden yang terjadi. Dengan demikian, UU KKS ini mengkolaborasikan secara komprehensif baik pendekatan hulu, menengah, maupun hilir.

Tujuan pembentukan UU KKS adalah untuk memberikan kepastian dan mengatur berbagai aspek Keamanan dan Ketahanan Siber di Indonesia untuk mendukung pertumbuhan ekonomi, ketertiban umum, dan pelayanan publik, dengan tetap mendorong inovasi teknologi dan pemanfaatannya untuk keunggulan negara.

II. PASAL DEMI PASAL

Pasal 1

Yang dimaksud merusak informasi melingkupi aspek kerahasiaan, keutuhan, otentikasi, nirsangkal, otorisasi, ketersediaan, dan akuntabilitas.

Pasal 2

Cukup Jelas

Pasal 3

Cukup Jelas.

Pasal 4

Cukup Jelas.

Pasal 5

Cukup Jelas.

Pasal 6

Cukup Jelas.

Pasal 7

Cukup Jelas

Pasal 8

Cukup Jelas.

Pasal 9

Cukup Jelas.

Pasal 10

Cukup Jelas.

Pasal 11

Cukup Jelas.

Pasal 12

Ayat (1)

Cukup Jelas.

Ayat (2)

Yang dimaksud dengan ”sertifikat” adalah sertifikat yang diterbitkan dengan berbasis algoritma kriptografi untuk menjadi penanda atau identitas digital dari orang, komputer, Sistem Elektronik, data, dokumen elektronik, dan/atau jaringan Siber.

Ayat (3)

Cukup Jelas.

Pasal 13

Ayat (1)

Yang dimaksud dengan “inklusivitas” adalah Penyelenggaraan Kecerdasan Artifisial perlu memperhatikan nilai kesetaraan, keadilan, dan perdamaian dalam menghasilkan informasi maupun inovasi untuk kepentingan bersama.

Yang dimaksud dengan “kemanusiaan” adalah Penyelenggaraan Kecerdasan Artifisial perlu memperhatikan nilai kemanusiaan dengan tetap saling menjaga hak asasi manusia, hubungan sosial, kepercayaan yang dianut, serta pendapat atau pemikiran setiap orang.

Yang dimaksud dengan “keamanan” adalah Penyelenggaraan Kecerdasan Artifisial perlu memperhatikan aspek keamanan pengguna dan data yang digunakan agar dapat menjaga privasi, data

pribadi, dan mengutamakan hak pengguna Sistem Elektronik sehingga tidak ada pihak yang dirugikan.

Yang dimaksud dengan "aksesibilitas" adalah Penyelenggaraan Kecerdasan Artifisial bersifat inklusif dan tidak diskriminatif. Setiap pengguna memiliki hak yang sama dalam mengakses penyelenggaraan teknologi berbasis Kecerdasan Artifisial untuk kepentingannya dengan tetap menjaga prinsip etika Kecerdasan Artifisial yang berlaku.

Yang dimaksud dengan "transparansi" adalah Penyelenggaraan Kecerdasan Artifisial perlu dilandasi dengan transparansi data yang digunakan untuk menghindari penyalahgunaan data dalam mengembangkan inovasi teknologi. Pelaku Usaha dan Penyelenggara Infrastruktur Informasi dapat memberikan akses kepada pengguna yang berhak untuk mengetahui penyelenggaraan data dalam pengembangan teknologi berbasis Kecerdasan Artifisial.

Yang dimaksud dengan "kredibilitas dan akuntabilitas" adalah Penyelenggaraan Kecerdasan Artifisial perlu mengutamakan kemampuan dalam pengambilan Keputusan dari informasi atau inovasi yang dihasilkan. Informasi yang dihasilkan melalui Kecerdasan Artifisial harus dapat dipercaya dan dipertanggungjawabkan ketika disebarkan kepada publik.

Yang dimaksud dengan "pelindungan data pribadi" adalah Penyelenggaraan Kecerdasan Artifisial harus memastikan pelindungan data pribadi sesuai ketentuan peraturan perundang-undangan.

Yang dimaksud dengan "pembangunan dan lingkungan berkelanjutan" adalah Penyelenggaraan Kecerdasan Artifisial mempertimbangkan dengan cermat dampak yang ditimbulkan terhadap manusia, lingkungan, dan makhluk hidup lainnya, untuk mencapai keberlanjutan dan kesejahteraan sosial.

Yang dimaksud dengan "pelindungan kekayaan intelektual" adalah Penyelenggaraan Kecerdasan Artifisial tunduk pada prinsip pelindungan Hak Kekayaan Intelektual sesuai ketentuan peraturan perundang-undangan.

Ayat (2)

Cukup Jelas.

Pasal 14

Cukup Jelas

Pasal 15

Cukup Jelas.

Pasal 16

Cukup Jelas.

Pasal 17

Cukup Jelas

Pasal 18

Cukup Jelas

Pasal 19

Cukup Jelas

Pasal 20

Cukup Jelas.

Pasal 21

Cukup Jelas

Pasal 22

Cukup Jelas

Pasal 23

Cukup Jelas

Pasal 24

Cukup Jelas.

Pasal 25

Huruf a

Yang dimaksud dengan “jaringan internet” adalah semua jenis jaringan yang memungkinkan konektivitas internet.

Huruf b

Yang dimaksud dengan “pusat data” adalah semua jenis jaringan yang memungkinkan konektivitas internet.

huruf c

Yang dimaksud dengan “data elektronik” adalah mencakup semua jenis data yang diproses, disimpan, dan dikirimkan secara elektronik.

huruf d

Yang dimaksud dengan “komputasi awan” atau cloud computing adalah teknologi yang memungkinkan pengguna untuk mengakses berbagai layanan komputasi, seperti penyimpanan data, aplikasi, pengelolaan basis data, jaringan, dan daya pemrosesan, melalui internet tanpa perlu memiliki infrastruktur fisik sendiri

huruf e

Yang dimaksud dengan “Sistem Elektronik” adalah perangkat keras, perangkat lunak, dan jaringan yang digunakan untuk mengolah data elektronik.

huruf f

Cukup Jelas.

huruf g

Cukup Jelas.

huruf h

Cukup Jelas.

Pasal 26

Cukup Jelas.

Pasal 27

Cukup Jelas.

Pasal 28

Cukup Jelas

Pasal 29

Cukup Jelas.

Pasal 30

Cukup Jelas.

Pasal 31

Ayat (1)

Kriptografi bertujuan meningkatkan derajat kepercayaan pada Sistem Elektronik yang lebih tinggi, yang diterapkan untuk memenuhi layanan keamanan yang meliputi aspek kerahasiaan, keutuhan, otentikasi, nirsangkal, otorisasi, ketersediaan, dan akuntabilitas.

Ayat (2)
Cukup Jelas.
Ayat (3)
Cukup Jelas.
Ayat (4)
Cukup Jelas.
Ayat (5)
Cukup Jelas.
Ayat (6)
Cukup Jelas.

Pasal 32
Cukup Jelas.

Pasal 33
Cukup Jelas.

Pasal 34
Cukup Jelas.

Pasal 35
Cukup Jelas.

Pasal 36
Cukup Jelas.

Pasal 37
Cukup Jelas

Pasal 38
Cukup Jelas.

Pasal 39
Cukup Jelas.

Pasal 40
Cukup Jelas.

Pasal 41
Cukup Jelas.

Pasal 42
Cukup Jelas.

Pasal 43
Cukup Jelas.

Pasal 44
Ayat (1)
Yang dimaksud “penindakan” adalah penindakan secara administratif.
Ayat (2)
Cukup Jelas.

Pasal 45
Cukup Jelas.

Pasal 46
Cukup Jelas.

Pasal 47
Cukup Jelas.

Pasal 48
Cukup Jelas.

Pasal 49
Cukup Jelas.

Pasal 50

Cukup Jelas.

Pasal 51

Ayat (1)

Cukup Jelas.

Ayat (2)

Cukup Jelas.

Ayat (3)

Huruf a

Cukup Jelas

Huruf b

Cukup Jelas

Huruf c

Yang dimaksud dengan “manajemen Krisis Siber” adalah tata kelola penggunaan sumber daya dan langkah penanganan secara efektif yang dilakukan sebelum, saat, dan setelah terjadinya Krisis Siber.

Huruf d

Cukup Jelas.

Pasal 52

Cukup Jelas.

Pasal 53

Cukup Jelas.

Pasal 54

Cukup Jelas.

Pasal 55

Cukup Jelas.

Pasal 56

Cukup Jelas.

Pasal 57

Cukup Jelas.

Pasal 58

Cukup Jelas.

Pasal 59

Cukup Jelas.

Pasal 60

Cukup Jelas.

Pasal 61

Cukup Jelas.

Pasal 62

Cukup Jelas.

Pasal 63

Cukup Jelas.

Pasal 64

Cukup Jelas.

Pasal 65

Cukup Jelas.

Pasal 66

Cukup Jelas.

Pasal 67

Cukup Jelas.

Pasal 68

Cukup Jelas.

Pasal 69

huruf a

Yang dimaksud dengan “menyelenggarakan fungsi Keamanan dan Ketahanan Siber” termasuk membentuk unit organisasi struktural di daerah dan/atau perwakilan di luar negeri.

huruf b

Cukup Jelas.

huruf c

Cukup Jelas.

huruf d

Cukup Jelas.

huruf e

Cukup Jelas.

huruf f

Cukup Jelas.

Pasal 70

Cukup Jelas.

Pasal 71

Cukup Jelas.

Pasal 72

Cukup Jelas.

Pasal 73

Cukup Jelas.

Pasal 74

Cukup Jelas.

Pasal 75

Cukup Jelas.

Pasal 76

Cukup Jelas.

Pasal 77

Cukup Jelas.

Pasal 78

Cukup Jelas.

Pasal 79

Cukup Jelas.

Pasal 80

Cukup Jelas.

Pasal 81

Cukup Jelas.

Pasal 82

Cukup Jelas.

Pasal 83

Cukup Jelas.

Pasal 84

Cukup Jelas.

Pasal 85

Cukup Jelas.

Pasal 86

Cukup Jelas.

Pasal 87

Cukup Jelas.

Pasal 88

Cukup Jelas.

Pasal 89

Cukup Jelas.

Pasal 90

Cukup Jelas.

Pasal 91

Cukup Jelas

Pasal 92

Cukup Jelas.

Pasal 93

Cukup Jelas.

Pasal 94

Cukup Jelas.

Pasal 95

Cukup Jelas.

Pasal 96

Cukup Jelas.

Pasal 97

Cukup Jelas.

Pasal 98

Cukup Jelas.

Pasal 99

Yang dimaksud dengan “deepfake” adalah teknik untuk sintesis citra manusia menggunakan kecerdasan artifisial (AI) yang outputnya dapat berupa gambar, rekaman video atau audio.

Pasal 100

Cukup Jelas.

Pasal 101

Cukup Jelas.

Pasal 102

Cukup Jelas.

Pasal 103

Cukup Jelas

Pasal 104

Cukup Jelas.

Pasal 105

Cukup Jelas.

Pasal 106

Cukup Jelas.