PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2023
TENTANG
KERANGKA KERJA PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 7 ayat (4) Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital;

Mengingat :
1. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
2. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
3. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Struktur Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG KERANGKA KERJA PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:
1. Kerangka Kerja Pelindungan Infrastruktur Informasi Vital yang selanjutnya disebut Kerangka Kerja adalah seperangkat konsep dasar yang digunakan sebagai

pedoman dalam menyusun, menerapkan, dan mengomunikasikan, aktivitas pengelolaan keamanan siber pada lingkup sektor infrastruktur informasi vital.

2. Infrastruktur Informasi Vital yang selanjutnya disingkat IIV adalah sistem elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan sistem elektronik lainnya dalam menunjang 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.
3. Penyelenggara IIV adalah instansi penyelenggara negara, badan usaha, dan/atau organisasi yang memiliki dan/atau mengoperasikan IIV.
4. Peristiwa Siber adalah kejadian pada sistem elektronik yang dapat diobservasi dan dapat memberikan indikasi terhadap terjadinya Insiden Siber.
5. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya sistem elektronik.
6. Kontrol Keamanan adalah tindakan pengendalian yang dilakukan oleh Penyelenggara IIV dalam mengelola risiko keamanan siber yang bentuknya dapat bersifat administratif, teknis, kebijakan manajemen, atau peraturan.
7. Instansi Penyelenggara Negara adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan.
8. Kementerian atau Lembaga adalah instansi penyelenggara negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya.
9. Badan Siber dan Sandi Negara yang selanjutnya disebut Badan adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi.

Pasal 2

Pengaturan Kerangka Kerja bertujuan untuk:

a. memberikan pedoman bagi Penyelenggara IIV dalam penyelenggaraan pelindungan IIV pada organisasinya; dan
b. menjadi acuan bagi Kementerian atau Lembaga dalam menyusun dan menetapkan peta jalan pelindungan IIV di masing-masing sektor IIV.

Pasal 3

Ruang lingkup pada Kerangka Kerja meliputi:

a. penyelenggaraan pelindungan IIV;
b. pembinaan dan pengawasan; dan
c. teknologi pelindungan IIV.

BAB II
PENYELENGGARAAN PELINDUNGAN IIV

Bagian Kesatu
Domain pada Kerangka Kerja

Pasal 4

(1) Penyelenggaraan pelindungan IIV sebagaimana dimaksud dalam Pasal 3 huruf a merupakan serangkaian upaya yang dilakukan oleh Penyelenggara IIV untuk mengendalikan keamanan melalui penerapan Kontrol Keamanan pada IIV sesuai dengan domain pada Kerangka Kerja.
(2) Domain pada Kerangka Kerja sebagaimana dimaksud pada ayat (1) meliputi:
    a. identifikasi;
    b. proteksi;
    c. deteksi; dan
    d. penanggulangan dan pemulihan.

Pasal 5

(1) Domain identifikasi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam memahami konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV.
(2) Domain identifikasi sebagaimana dimaksud pada ayat (1) terdiri atas kategori kegiatan paling sedikit:
    a. mengidentifikasi peran dan tanggung jawab organisasi;
    b. menyusun strategi, kebijakan, dan prosedur pelindungan IIV;
    c. mengelola aset informasi;
    d. menilai dan mengelola risiko keamanan siber; dan
    e. mengelola risiko rantai pasok.
(3) Kategori kegiatan mengidentifikasi peran dan tanggung jawab organisasi sebagaimana dimaksud pada ayat (2) huruf a terdiri atas subkategori kegiatan paling sedikit:
    a. menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan IIV di organisasi;
    b. mengidentifikasi ketergantungan organisasi dengan pihak terkait lainnya; dan
    c. mengidentifikasi dan mengomunikasikan peran organisasi di dalam sektor IIV.
(4) Kategori kegiatan menyusun strategi, kebijakan, dan prosedur pelindungan IIV sebagaimana dimaksud pada ayat (2) huruf b terdiri atas subkategori kegiatan paling sedikit:
    a. menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan Penyelenggara IIV;
    b. mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV;
    c. menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan;
    d. menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga.

(5) Kategori kegiatan mengelola aset informasi sebagaimana dimaksud pada ayat (2) huruf c terdiri atas subkategori kegiatan paling sedikit:
   a. mengelola daftar inventaris aset informasi;
   b. memetakan jalur komunikasi dan alur data pada organisasi;
   c. menyusun katalog sistem informasi eksternal yang menggunakan data milik organisasi;
   d. menyusun prioritas aset informasi berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya; dan
   e. mengendalikan aset informasi milik organisasi.

(6) Kategori kegiatan menilai dan mengelola risiko keamanan siber sebagaimana dimaksud pada ayat (2) huruf d terdiri atas subkategori kegiatan paling sedikit:
   a. mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi;
   b. mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal;
   c. mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut;
   d. menganalisis nilai risiko terhadap IIV;
   e. mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko;
   f. menentukan dan mengomunikasikan toleransi risiko organisasi;
   g. mengelola hasil penerapan manajemen risiko yang telah ditetapkan; dan
   h. melakukan reviu terhadap hasil penerapan manajemen risiko.

(7) Kategori kegiatan mengelola risiko rantai pasok sebagaimana dimaksud pada ayat (2) huruf e terdiri atas subkategori kegiatan paling sedikit:
   a. mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok;
   b. mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV;
   c. memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV;
   d. melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya; dan
   e. menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut.

Pasal 6

(1) Domain proteksi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam mencegah, membatasi, atau menahan dampak dari Insiden Siber.

(2) Domain proteksi sebagaimana dimaksud pada ayat (1) terdiri atas kategori kegiatan paling sedikit:

a. mengelola identitas, autentikasi, dan kendali akses;
b. melindungi aset fisik;
c. melindungi data;
d. melindungi aplikasi;
e. melindungi jaringan; dan
f. melindungi sumber daya manusia.

(3) Kategori kegiatan mengelola identitas, autentikasi, dan kendali akses sebagaimana dimaksud pada ayat (2) huruf a terdiri atas subkategori kegiatan paling sedikit:
a. mengelola identitas dan kredensial yang menggunakan layanan IIV;
b. mengelola akses jarak jauh terhadap layanan IIV;
c. mengelola izin akses dan otorisasi layanan IIV; dan
d. memastikan penerapan sistem autentikasi terhadap pengguna, perangkat, dan aset informasi sesuai tingkat risikonya.

(4) Kategori kegiatan melindungi aset fisik sebagaimana dimaksud pada ayat (2) huruf b terdiri atas subkategori kegiatan paling sedikit:
a. menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV;
b. memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur;
c. memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur;
d. memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman; dan
e. memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman.

(5) Kategori kegiatan melindungi data sebagaimana dimaksud pada ayat (2) huruf c terdiri atas subkategori kegiatan paling sedikit:
a. pelindungan terhadap data yang tersimpan pada Penyelenggara IIV;
b. pelindungan terhadap data yang terkirim dari Penyelenggara IIV;
c. memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai;
d. mengimplementasikan pelindungan dari kebocoran data;
e. mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data;
f. memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala; dan
g. menyediakan kebijakan pemusnahan data.

(6) Kategori kegiatan melindungi aplikasi sebagaimana dimaksud pada ayat (2) huruf d terdiri atas subkategori kegiatan paling sedikit:
a. menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi;

b. mengembangkan dan mengimplementasikan rencana manajemen kerentanan;
c. memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional; dan
d. mengimplementasikan prosedur pengembangan sistem yang aman.

(7) Kategori kegiatan melindungi jaringan sebagaimana dimaksud pada ayat (2) huruf e terdiri atas subkategori kegiatan paling sedikit:
a. menerapkan sistem yang dikonfigurasi dengan prinsip fungsionalitas minimum;
b. menerapkan pelindungan terhadap jaringan komunikasi, akses sistem informasi, dan akses sistem kendali;
c. menggunakan perangkat-perangkat jaringan yang menerapkan fungsi keamanan;
d. memastikan integritas jaringan senantiasa dilindungi;
e. menerapkan prosedur dan teknologi pencegahan *malware*;
f. memastikan catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan organisasi; dan
g. memastikan bahwa informasi mengenai pelindungan terhadap teknologi dibagikan hanya kepada pihak tepercaya.

(8) Kategori kegiatan melindungi sumber daya manusia sebagaimana dimaksud pada ayat (2) huruf f terdiri atas subkategori kegiatan paling sedikit:
a. menerapkan prosedur pengelolaan keamanan terhadap personel;
b. menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber; dan
c. menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di Penyelenggara IIV.

Pasal 7

(1) Domain deteksi sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf c merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam mengembangkan dan menerapkan aktivitas yang sesuai untuk memantau secara tepat waktu terjadinya Peristiwa Siber.

(2) Domain deteksi sebagaimana dimaksud pada ayat (1) terdiri atas kategori kegiatan paling sedikit:
a. mengelola deteksi Peristiwa Siber;
b. menganalisis anomali dan Peristiwa Siber; dan
c. memantau Peristiwa Siber berkelanjutan.

(3) Kategori kegiatan mengelola deteksi Peristiwa Siber sebagaimana dimaksud pada ayat (2) huruf a terdiri atas subkategori kegiatan paling sedikit:
a. menetapkan peran dan tanggung jawab organisasi pada kebijakan pendeteksian Peristiwa Siber;

b. melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku;
c. menguji prosedur pendeteksian Peristiwa Siber secara berkala; dan
d. menyampaikan informasi hasil pendeteksian Peristiwa Siber kepada pihak yang berhak.

(4) Kategori kegiatan menganalisis anomali dan Peristiwa Siber sebagaimana dimaksud pada ayat (2) huruf b terdiri atas subkategori kegiatan paling sedikit:
a. menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data;
b. melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi;
c. menentukan dampak dari Peristiwa Siber yang terdeteksi; dan
d. mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi.

(5) Kategori kegiatan memantau Peristiwa Siber berkelanjutan sebagaimana dimaksud pada ayat (2) huruf c terdiri atas subkategori kegiatan paling sedikit:
a. menerapkan prosedur pendeteksi kode berbahaya dan tak berizin;
b. memonitor kegiatan personel yang berada di dalam lingkup sistem IIV;
c. memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV; dan
d. menerapkan teknologi pemindaian kerentanan terhadap sistem IIV.

Pasal 8

(1) Domain penanggulangan dan pemulihan sebagaimana dimaksud dalam Pasal 4 ayat (3) huruf d merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV dalam menyusun dokumen rencana penanggulangan dan pemulihan Insiden Siber, menerapkan aktivitas yang sesuai untuk mengambil tindakan terkait Insiden Siber yang terdeteksi, menahan meluasnya dampak dari Insiden Siber, memulihkan layanan yang terganggu karena Insiden Siber, serta mengurangi dampak dari Insiden Siber.

(2) Domain penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) terdiri atas kategori kegiatan paling sedikit:
a. menyusun perencanaan penanggulangan dan pemulihan Insiden Siber;
b. menganalisis dan melaporkan Insiden Siber;
c. melaksanakan penanggulangan dan pemulihan Insiden Siber; dan
d. meningkatkan keamanan setelah terjadinya Insiden Siber.

(3) Kategori kegiatan menyusun perencanaan penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf a terdiri atas subkategori kegiatan paling sedikit:

a. menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi;
b. menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi;
c. memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala;
d. memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan; dan
e. memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang.

(4) Kategori kegiatan menganalisis dan melaporkan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf b terdiri atas subkategori kegiatan paling sedikit:
a. mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal~~,~~ maupun sumber informasi eksternal;
b. mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber;
c. memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan; dan
d. memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait.

(5) Kategori kegiatan melaksanakan penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf c terdiri atas subkategori kegiatan paling sedikit:
a. memastikan Insiden Siber diisolasi dan dimitigasi sesuai rencana tanggap Insiden Siber;
b. mengumpulkan dan memelihara bukti Insiden Siber dari IIV terdampak;
c. menginvestigasi dan eradikasi penyebab Insiden Siber;
d. mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan Insiden Siber.
e. memastikan setiap aset informasi diperiksa keamanannya setelah penanganan Insiden Siber;
f. melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan;
g. menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan;
h. pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi;
i. memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi Insiden Siber dan setelah penanggulangan serta pemulihan Insiden Siber; dan
j. penyampaian informasi penanggulangan dan pemulihan Insiden Siber kepada pihak terkait.

(6) Kategori kegiatan meningkatkan keamanan setelah terjadinya Insiden Siber sebagaimana dimaksud pada ayat (2) huruf d terdiri atas subkategori kegiatan paling sedikit:
   a. meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan;
   b. mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala;
   c. mengumpulkan dan memelihara bukti hasil forensik digital; dan
   d. meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala.

Pasal 9

Penerapan Kontrol Keamanan sebagaimana dimaksud dalam Pasal 4 ayat (1) dilakukan sesuai dengan matriks Kerangka Kerja sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 10

Selain kategori dan subkategori kegiatan pada domain Kerangka Kerja sebagaimana dimaksud dalam Pasal 5 sampai dengan Pasal 8, Kementerian atau Lembaga dapat menambahkan kategori dan subkategori kegiatan lainnya sesuai dengan karakteristik sektornya dengan memperhatikan prinsip keamanan, keandalan, dan efisiensi.

Bagian Kedua
Penerapan Kerangka Kerja

Pasal 11

(1) Kementerian atau Lembaga menyusun dan menetapkan peta jalan pelindungan IIV di masing-masing sektor IIV untuk jangka waktu 5 (lima) tahun mengacu pada Kerangka Kerja pelindungan IIV.
(2) Peta jalan pelindungan IIV sebagaimana dimaksud pada ayat (1) dimaksudkan untuk memberi arah dan langkah perencanaan serta pelaksanaan bagi Penyelenggara IIV dalam menyelenggarakan pelindungan IIV di masing-masing sektor IIV.
(3) Peta jalan pelindungan IIV sebagaimana dimaksud pada ayat (1) memuat:
   a. analisis lingkungan strategis penyelenggaraan pelindungan IIV di masing-masing sektor (*current profile*);
   b. arah kebijakan penyelenggaraan pelindungan IIV;
   c. sasaran penyelenggaraan pelindungan IIV;
   d. target penerapan Kontrol Keamanan; dan
   e. rencana kerja penyelenggaraan pelindungan IIV.

Pasal 12

(1) Analisis lingkungan strategis penyelenggaraan pelindungan IIV sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf a dimaksudkan untuk memberi gambaran

kondisi penerapan Kontrol Keamanan saat ini di masing-masing sektor IIV.

(2) Analisis lingkungan strategis penyelenggaraan pelindungan IIV sebagaimana dimaksud pada ayat (1) dilaksanakan dengan kegiatan paling sedikit:
   a. mendeskripsikan layanan vital di sektor IIV dan sistem elektronik yang menunjang layanan tersebut;
   b. analisis dampak yang mungkin timbul dari gangguan terhadap layanan vital dan sistem elektronik tersebut;
   c. identifikasi regulasi nasional dan/atau internasional yang terkait dalam operasional layanan vital tersebut;
   d. identifikasi kegiatan pelindungan yang telah diterapkan pada layanan vital dari aspek ketersediaan dan kemampuan sumber daya manusia, tata kelola, dan teknologi; dan/atau
   e. analisis kesenjangan antara kondisi penerapan Kontrol Keamanan saat ini dan kondisi penerapan yang ingin dicapai.

Pasal 13

(1) Arah kebijakan pelindungan IIV pada peta jalan pelindungan IIV sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf b dimaksudkan untuk memberi arahan kepada Penyelenggara IIV mengenai kebijakan prioritas yang akan diterapkan di masing-masing sektor.

(2) Arah kebijakan pelindungan IIV sebagaimana dimaksud pada ayat (1) dapat berisi strategi yang meliputi:
   a. pemenuhan atau peningkatan kemampuan sektor dalam mengidentifikasi konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV di sektornya;
   b. pemenuhan atau peningkatan kemampuan sektor dalam mencegah, membatasi, dan menahan dampak dari Insiden Siber;
   c. pemenuhan atau peningkatan kemampuan sektor dalam memantau secara tepat waktu terjadinya Peristiwa Siber; dan
   d. pemenuhan atau peningkatan kemampuan sektor dalam mengambil tindakan terkait penanggulangan dan pemulihan Insiden Siber.

Pasal 14

(1) Sasaran penyelenggaraan pelindungan IIV sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf c dimaksudkan untuk memberi arahan kepada Penyelenggara IIV mengenai tujuan spesifik yang akan dicapai dalam memenuhi arah kebijakan.

(2) Sasaran penyelenggaraan pelindungan IIV sebagaimana dimaksud pada ayat (1) dapat disusun berdasarkan kategori kegiatan yang ada pada domain Kerangka Kerja sebagaimana dimaksud dalam pasal 4 ayat (2).

Pasal 15

(1) Target penerapan Kontrol Keamanan sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf d merupakan nilai capaian yang bertujuan untuk memberikan gambaran

kondisi penerapan keamanan siber pada Penyelenggara IIV terhadap sasaran penyelenggaraan pelindungan IIV dan domain Kerangka Kerja sebagaimana dimaksud dalam Pasal 4 ayat (2).

(2) Target penerapan Kontrol Keamanan sebagaimana dimaksud pada ayat (1) ditentukan berdasarkan hasil pengukuran tingkat kematangan keamanan siber yang dibagi menjadi:
   a. level 1 (satu), dinamakan level awal;
   b. level 2 (dua), dinamakan level berulang;
   c. level 3 (tiga), dinamakan level terdefinisi;
   d. level 4 (empat), dinamakan level terkelola; dan
   e. level 5 (lima), dinamakan level inovatif.

(3) Target penerapan Kontrol Keamanan sebagaimana dimaksud pada ayat (2) ditentukan paling rendah pada level 3 (tiga) dari hasil pengukuran tingkat kematangan keamanan siber.

(4) Ketentuan mengenai pengukuran tingkat kematangan keamanan siber sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Badan tersendiri.

Pasal 16

(1) Rencana kerja penyelenggaraan pelindungan IIV sebagaimana dimaksud dalam Pasal 11 ayat (3) huruf e dimaksudkan untuk memberi arahan kepada Penyelenggara IIV, Kementrian atau Lembaga, atau pihak lainnya mengenai kegiatan yang harus dilakukan untuk mencapai sasaran penyelenggaraan pelindungan IIV sebagaimana dimaksud dalam Pasal 14 ayat (1).

(2) Rencana kerja penyelenggaraan pelindungan IIV sebagaimana dimaksud pada ayat (1) dapat disusun berdasarkan sub-kategori kegiatan sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 17

Penyusunan peta jalan pelindungan IIV sebagaimana dimaksud dalam Pasal 11 dituangkan dalam contoh format penyusunan peta jalan sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

BAB III
PEMBINAAN DAN PENGAWASAN

Bagian Kesatu
Pembinaan dan Pengawasan oleh Kementerian atau Lembaga

Pasal 18

(1) Kementerian atau Lembaga melakukan pembinaan dan pengawasan terhadap penyelenggaraan pelindungan IIV di sektornya sesuai dengan peta jalan pelindungan IIV sebagaimana dimaksud dalam Pasal 11.

(2) Pembinaan sebagaimana dimaksud pada ayat (1) berupa kegiatan:
   a. mengoordinasikan peningkatan kapasitas sumber daya manusia yang ada di masing-masing sektor IIV;

b. penyelenggaraan kegiatan simulasi tanggap Insiden Siber untuk lingkup sektor yang diikuti oleh seluruh Penyelenggara IIV di masing-masing sektor IIV;
c. penyelenggaraan forum analisis dan berbagi informasi keamanan siber dalam lingkup sektornya;
d. koordinasi teknis penyelenggaraan pelindungan IIV dalam lingkup sektor IIV; dan/atau
e. kegiatan lain yang dibutuhkan oleh Penyelenggara IIV di masing-masing sektor IIV.

(3) Pengawasan terhadap penerapan penyelenggaraan pelindungan IIV sebagaimana yang dimaksud pada ayat (1) meliputi kegiatan:
a. menerima dan memverifikasi laporan penerapan peta jalan pelindungan IIV yang dilakukan oleh Penyelenggara IIV; dan
b. pemantauan dan evaluasi penerapan peta jalan pelindungan IIV yang dilakukan oleh Penyelenggara IIV hasil pengukuran tingkat kematangan keamanan siber yang dilaporkan oleh Penyelenggara IIV.

Bagian Kedua
Pembinaan dan Pengawasan oleh Badan

Pasal 19

(1) Pembinaan dan pengawasan penyelenggaraan pelindungan IIV secara nasional dilakukan oleh Badan dengan berkoordinasi kepada Kementerian atau Lembaga di masing-masing sektor IIV.
(2) Pembinaan yang dilakukan oleh Badan sebagaimana dimaksud pada ayat (1) berupa kegiatan:
a. mengoordinasikan peningkatan kapasitas sumber daya manusia keamanan siber dan sandi untuk seluruh sektor IIV;
b. bantuan teknis penerapan Kontrol Keamanan dan/atau pengujian keamanan siber;
c. penyelenggaraan kegiatan simulasi tanggap Insiden Siber untuk lingkup nasional yang dapat diikuti oleh seluruh Penyelenggara IIV dan Kementerian atau Lembaga;
d. penyelenggaraan forum analisis dan berbagi informasi keamanan siber dalam lingkup nasional;
e. koordinasi teknis penyelenggaraan pelindungan IIV dalam lingkup sektor IIV;dan/atau
f. kegiatan lain yang dibutuhkan oleh Penyelenggara IIV dalam rangka penyelenggaraan pelindungan IIV.

(3) Pengawasan yang dilakukan oleh Badan sebagaimana dimaksud pada ayat (1) meliputi kegiatan:
a. memonitor penyusunan peta jalan pelindungan IIV dan reviu terhadap peta jalan pelindungan IIV; dan
b. mengevaluasi implementasi kebijakan penyelenggaraan pelindungan IIV.

BAB IV
TEKNOLOGI PELINDUNGAN IIV

Bagian Kesatu
Perangkat Teknologi Pelindungan IIV

Pasal 20

(1) Teknologi pelindungan IIV merupakan perangkat teknologi pelindungan yang digunakan oleh Penyelenggara IIV untuk mendukung penerapan domain pada Kerangka Kerja.
(2) Teknologi pelindungan IIV sebagaimana dimaksud pada ayat (1) terdiri atas perangkat yang digunakan untuk mendukung domain pada Kerangka Kerja dengan fungsi:
    a. pengelolaan aset informasi;
    b. repositori manajemen konfigurasi;
    c. manajemen kapasitas (*capacity management*);
    d. manajemen kerentanan rantai pasok;
    e. pengujian keamanan sistem;
    f. manajemen kerentanan teknis;
    g. pencatatan *(logging);*
    h. pemantauan keamanan dan performa (*monitoring);*
    i. manajemen identitas dan/atau pengguna;
    j. pelindungan telekarya (*teleworking*);
    k. pengamanan pada transfer data/informasi;
    l. pemusnahan data dan media;
    m. pengelolaan media yang dapat dipindahkan (*removable media*);
    n. pengelolaan hak akses istimewa (*privileged access rights*);
    o. pengamanan terhadap akses ke jaringan dan layanan jaringan;
    p. pembatasan instalasi perangkat lunak;
    q. pengamanan layanan aplikasi di jaringan publik;
    r. kontrol akses ke kode sumber (*source code*);
    s. kriptografi;
    t. sistem kontrol terdistribusi;
    u. pengecekan integritas file (*file integrity monitoring*)
    v. pencegahan kebocoran data (*data loss prevention*)
    w. *backups (rekam cadang)* dan redudansi;
    x. pengelolaan insiden; atau
    y. fungsi lain yang dapat mendukung pelindungan IIV.

Bagian Kedua
Keamanan Perangkat Teknologi

Pasal 21

(1) Penyelenggara IIV wajib memastikan keamanan perangkat teknologi pelindungan IIV yang digunakan sebagaimana dimaksud dalam Pasal 20.
(2) Keamanan perangkat teknologi pelindungan IIV sebagaimana dimaksud pada ayat (1) dibuktikan dengan tanda sertifikasi.
(3) Terhadap tanda sertifikasi sebagaimana dimaksud pada ayat (2) dilakukan verifikasi dan/atau rekognisi oleh

Badan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
KETENTUAN PERALIHAN

Pasal 22

Penyelenggara IIV wajib memiliki tanda sertifikasi sebagaimana dimaksud dalam Pasal 21 ayat (2) paling lambat 24 (dua puluh empat) bulan terhitung sejak Peraturan Badan ini mulai berlaku.

BAB VI
KETENTUAN PENUTUP

Pasal 23

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Badan ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 16 Oktober 2023

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 3 November 2023

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd.

ASEP N. MULYANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2023 NOMOR 873

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2023
TENTANG
KERANGKA KERJA PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL

A. MATRIKS KERANGKA KERJA PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL

Matriks Kerangka Kerja Pelindungan Infrastruktur Informasi Vital (IIV) berisi daftar domain, kategori, sub-kategori, dan kontrol yang menguraikan spesifik kegiatan keamanan siber yang umum diselenggarakan dalam rangka pelindungan pada IIV. Format presentasi yang digambarkan pada matriks Kerangka Kerja ini bukan merupakan urutan pelaksanaan kegiatan, atau derajat kepentingan antar kegiatan, melainkan kumpulan kegiatan yang dapat dilaksanakan oleh penyelenggara IIV untuk menyelenggarakan keamanan siber di organisasinya.

Meskipun matriks Kerangka Kerja ini tidak menjabarkan kegiatan-kegiatan keamanan siber secara menyeluruh, namun matriks ini dapat diperluas sesuai kebutuhan dan kondisi yang ada. Sehingga, memungkinkan bagi penyelenggara IIV, Kementerian atau Lembaga di masing-masing sektor IIV, dan pemangku kepentingan lainnya menggunakan referensi informasi lainnya sesuai dengan standar atau praktik terbaik yang diacu oleh masing-masing sektor IIV. Kegiatan-kegiatan keamanan siber yang diperlukan untuk pelindungan IIV dapat dipilih dari matriks Kerangka Kerja ini dengan mengacu kepada manajemen risiko yang berlaku di penyelenggara IIV, dan persyaratan hukum/regulasi yang berlaku.

Tabel 1. Matriks Kerangka Kerja Pelindungan Infrastruktur Informasi Vital

Domain		**Kategori**		**Sub-Kategori**		**Kontrol**		**Ruang Lingkup**
1	Identifikasi	1.1	Mengidentifikasi peran dan tanggung jawab organisasi	1.1.1	Menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan IIV di organisasi	a.	Pimpinan organisasi menetapkan keamanan siber sebagai prioritas di organisasi dalam bentuk kebijakan atau komitmen pimpinan yang sesuai dengan kondisi bisnis/layanan dan operasional organisasi.	Tata Kelola
						b.	Penyelenggara IIV mengomunikasikan perihal komitmen keamanan siber di organisasnya dengan pihak-pihak yang terkait dengan bisnis/layanan organisasi (termasuk kepada penyedia pihak ketiga).	Tata Kelola
				1.1.2	Mengidentifikasi ketergantungan organisasi dengan pihak terkait lainnya	a.	Penyelenggara IIV mengidentifikasi unit kerja di internal organisasinya, maupun pihak lain di luar organisasinya yang memiliki ketergantungan, baik secara langsung maupun tidak langsung terhadap operasional layanan IIV di organisasinya.	Tata Kelola
				1.1.3	Mengidentifikasi dan mengomunikasikan peran organisasi di dalam sektor IIV	a	Penyelenggara IIV mengidentifikasi dan menetapkan unit kerja atau fungsi yang memiliki tugas dan tanggung jawab dalam menerapkan pelindungan IIV di organisasinya.	Tata Kelola
						b	Penyelenggara IIV mengidentifikasi peran, aktivitas, proses, dan narahubung dari	Tata Kelola

							pemangku kepentingan yang mendukung ekosistem bisnis atau layanan IIV, baik di dalam atau di luar organisasi.	
		1.2	Menyusun strategi, kebijakan, dan prosedur Pelindungan IIV	1.2.1	Menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan penyelenggara IIV	a	Penyelenggara IIV menyusun, menetapkan, dan mengembangkan kebijakan tentang keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan	Tata Kelola
						b	Penyelenggara IIV mengomunikasikan kebijakan kepada seluruh personel yang relevan, serta mengoordinasikan dan menyepakati metode berbagi informasi mengenai kebijakan dan prosedur yang ada di organisasi dengan para pemangku kepentingan eksternal.	Tata Kelola
						c	Penyelenggara IIV meninjau dan merevisi kebijakannya secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya.	Tata Kelola
				1.2.2	Mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV	a	Penyelenggara IIV senantiasa mengembangkan strategi dalam melindungi aset informasi dengan mempertimbangkan manajemen risiko yang berlaku di organisasi.	Tata Kelola
						b	Penyelenggara IIV harus menetapkan sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang	Tata Kelola

							relevan.	
				1.2.3	Menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan	a	Penyelenggara IIV menyusun kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung IIV baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber.	Tata Kelola
				1.2.4	Menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga	a	Penyelenggara IIV menyusun kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (*bring your own devices*), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi, dsb.	Tata Kelola
		1.3	Mengelola aset informasi	1.3.1	Mengelola daftar inventaris aset informasi	a	Dokumentasikan dan kelola dengan tepat daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb).	Tata Kelola & Teknologi
						b	Penyelenggara IIV memastikan pemberian label pada perangkat aset informasi oleh pihak yang berwenang di organisasi.	Tata Kelola
				1.3.2	Memetakan jalur komunikasi dan alur data pada organisasi	a	Penyelenggara IIV menyusun dokumentasi dan mengelola diagram jalur komunikasi jaringan dan aliran data dengan tepat dalam organisasi.	Teknologi

				1.3.3	Menyusun katalog sistem informasi eksternal yang menggunakan data milik organisasi	a	Dokumentasikan dan kelola dengan tepat daftar sistem informasi eksternal yang menggunakan data atau layanan IIV.	Tata Kelola
						b	Dokumentasikan dan kelola dengan tepat daftar sistem informasi eksternal yang digunakan oleh penyelenggara IIV.	Tata Kelola
				1.3.4	Menyusun prioritas aset informasi berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya	a	Mengklasifikasikan dan memprioritaskan aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisan, dan nilai bisnis.	Tata Kelola
				1.3.5	Mengendalikan aset informasi milik organisasi	a	Menentukan metode untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait.	Tata Kelola & Teknologi
						b	Secara aktif memeriksa keterbaharuan dan memperbaharui dari setiap versi perangkat lunak dan perangkat keras yang digunakan oleh organisasi.	Teknologi
		1.4	Menilai dan mengelola risiko Keamanan Siber	1.4.1	Mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi.	a	Identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui *penetration testing* dan *vulnerability assessment*, serta dokumentasikan daftar kerentanan yang	Teknologi

							teridentifikasi tersebut bersama dengan daftar aset terkait.	
				1.4.2	Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal	a	Penyelenggara IIV mengumpulkan informasi termasuk kerentanan dan ancaman dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.)	Teknologi & Tata Kelola
						b	Menganalisis informasi tersebut apakah termasuk kedalam konteks risiko terhadap aset informasi, dan mendokumentasikannya.	Tata Kelola
				1.4.3	Mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut	a	Penyelenggara IIV perlu memeriksa pada setiap fungsi penting organisasi apakah ada risiko keamanan yang diketahui termasuk kedalam kategori membahayakan keselamatan, menimbulkan kerugian, dan mengancam keamanan negara.	Tata Kelola
				1.4.4	Menganalisis nilai risiko terhadap IIV	a	Pertimbangkan ancaman, kerentanan, kemungkinan, dan dampak saat menganalisis risiko.	Tata Kelola
						b	Penyelenggara IIV menentukan level risiko dan prioritas mitigasinya.	Tata Kelola

				1.4.5	Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko	a	Berdasarkan hasil penilaian risiko, tentukan dengan jelas rincian tindakan untuk mencegah kemungkinan risiko keamanan, dan dokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan.	Tata Kelola
						b	Evaluasi hasil penerapan respon risiko secara berkelanjutan.	Tata Kelola
				1.4.6	Menentukan dan mengomunikasikan toleransi risiko organisasi	a	Menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku.	Tata Kelola
				1.4.7	Mengelola hasil penerapan manajemen risiko yang telah ditetapkan	a	Konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan komunikasikan hasilnya kepada pihak yang tepat di dalam organisasi (misalnya pimpinan organisasi).	Tata Kelola
						b	tetapkan serta terapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait.	Tata Kelola
				1.4.8	Melakukan reviu terhadap hasil penerapan manajemen risiko	a	Penyelenggara IIV melakukan reviu terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko.	Tata Kelola
		1.5	Mengelola risiko rantai pasok	1.5.1	Mengidentifikasi dan menetapkan proses	a	Merumuskan standar tindakan keamanan yang relevan dengan rantai	Tata Kelola

					manajemen risiko rantai pasok		pasokan dan menyepakati konten dengan mitra bisnis setelah memperjelas ruang lingkup tanggung jawab masing-masing.	
						b	hal yang perlu dipertimbangkan dalam proses manajemen risiko rantai pasokan diantaranya adalah penentuan jenis akses yang diberikan, alasan kebutuhan akses, metode akses, jangka waktu, dan potensi risiko yang terjadi apabila akses tersebut disalahgunakan.	Tata Kelola
				1.5.2	Mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV	a	identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan dengan penyelenggara IIV.	Tata Kelola
						b	Merumuskan dan mengelola persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga.	Tata Kelola
				1.5.3	Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra	a	Saat menandatangani kontrak dengan pihak ketiga, periksa apakah manajemen pihak ketiga telah dengan benar mematuhi persyaratan keamanan,	Tata Kelola

					pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV		standar, dan peraturan perundangan yang berlaku, dengan mempertimbangkan tujuan kontrak tersebut dan hasil manajemen risiko.	
						b	Saat menandatangani kontrak dengan pihak ketiga, periksa apakah produk dan layanan yang disediakan oleh pihak ketiga sesuai dengan persyaratan keamanan yang ada di organisasi.	Tata Kelola
				1.5.4	Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya	a	Melakukan penilaian secara berkala melalui audit, hasil pengujian, atau pemeriksaan dari pihak terkait untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka.	Tata Kelola
						b	Merumuskan dan menerapkan prosedur untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan.	Tata Kelola
						c	Mengumpulkan dan menyimpan data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum.	Tata Kelola
				1.5.5	Menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang	a	Menyiapkan dan menguji prosedur respons insiden dengan pihak terkait yang terlibat dalam aktivitas respons insiden untuk memastikan tindakan respons dilaksanakan dalam rantai	Tata Kelola

					mendukung layanan tersebut		pasokan.	
						b	menyusun prosedur keamanan yang akan dijalankan ketika kontrak dengan pihak ketiga selesai. (misalnya, pemutusan hak akses ketika berakhirnya masa kontrak)	Tata Kelola
						c	senantiasa meningkatkan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok.	Tata Kelola
2	Proteksi	2.1	Mengelola identitas, autentikasi, dan kendali akses	2.1.1	Mengelola identitas dan kredensial yang menggunakan layanan IIV	a	Menetapkan dan menerapkan prosedur untuk menerbitkan, mengelola, memeriksa, membatalkan, dan memantau informasi tentang identitias dan kredensial terhadap aset informasi dan personel yang menggunakan IIV.	Tata Kelola & teknologi
				2.1.2	Mengelola akses jarak jauh terhadap layanan IIV	a	Penyelenggara IIV menyusun prosedur tentang mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan, termasuk pemberian koneksi terhadap pengguna, perangkat IoT, dan/atau server.	Tata Kelola & Teknologi
						b	tersedianya dan diterapkannya prosedur pencegahan terhadap upaya memasuki perangkat atau jaringan secara tidak sah, dengan menerapkan langkah-langkah seperti menerapkan fungsi untuk	Teknologi

							penguncian setelah sejumlah upaya masuk yang gagal dan memberikan interval waktu hingga keamanannya dipastikan.	
				2.1.3	Mengelola izin akses dan otorisasi layanan IIV	a	Menyusun dan menerapkan prosedur untuk memisahkan hak akses sesuai tugas dan area tanggung jawab (misalnya, pisahkan fungsi untuk pengguna dari fungsi untuk administrator sistem)	Tata Kelola & teknologi
						b	tersedianya prosedur pembatasan komunikasi oleh perangkat dan server kepada pengguna sesuai dengan tingkat risikonya.	Teknologi
				2.1.4	Memastikan penerapan sistem autentikasi terhadap pengguna, perangkat, dan aset informasi sesuai tingkat risikonya	a	perangkat, pengguna, dan aset informasi lainnya menggunakan sistem otentikasi tertentu (misalnya, multi-factor authentication) sesuai dengan tingkat risiko nya terhadap sistem.	Tata Kelola & Teknologi
		2.2	Melindungi aset fisik	2.2.1	Menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV	a	menetapkan dan menerapkan prosedur keamanan fisik terhadap akses kontrol yang sesuai seperti mengunci dan membatasi akses ke area tempat perangkat dan server dipasang, menggunakan kontrol masuk dan keluar, otentikasi biometrik, memasang kamera	Tata Kelola & teknologi

							pengintai, dan/atau memeriksa barang bawaan.	
						b	Tersedianya dan diterapkannya prosedur pelindungan fisik seperti menyiapkan catu daya cadangan, fasilitas proteksi kebakaran, dan perlindungan dari resapan air yang mengikuti kebijakan dan standar yang berlaku.	Tata Kelola
						c	Tersedianya prosedur dan sarana pengamanan terhadap perangkat komputer yang digunakan untuk pengolahan data IIV.	Tata Kelola & Teknologi
				2.2.2	Memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur	a	Tentukan metode untuk melakukan pembaruan keamanan dan sejenisnya pada perangkat dan server. Kemudian, terapkan pembaruan keamanan tersebut dengan teknologi yang benar dan tepat pada waktunya.	Tata Kelola & Teknologi
						b	Dokumentasikan kegiatan pembaruan keamanan pada perangkat organisasi dan laporkan kepada manajemen secara berkala.	Tata Kelola
				2.2.3	Memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan	a	Mengidentifikasi perangkat yang memiliki mekanisme pembaruan jarak jauh untuk melakukan pembaruan massal berbagai program perangkat lunak (OS, driver, dan aplikasi) melalui perintah jarak jauh.	Teknologi
						b	Melakukan pemeliharaan perangkat dan server yang telah disetujui dari jarak jauh dan mencatat setiap log masuknya,	Teknologi

					sesuai prosedur		sehingga akses yang tidak sah dapat dicegah.	
				2.2.4	Memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman	a	Penyelenggara IIV memastikan lingkungan fisik aset IIV dipantau secara tepat melalui pengaturan, perekaman, dan pemantauan akses fisik terhadap aset IIV. (misalnya cctv, akses kontrol, sensor, dll).	Teknologi
				2.2.5	Memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman	a	Penyelenggara IIV senantiasa melakukan peninjauan, analisis, dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil reviu dari respons insiden keamanan dan hasil pemantauan, pengukuran, dan evaluasi ancaman internal dan eksternal.	Tata Kelola
		2.3	Melindungi data	2.3.1	Pelindungan terhadap data yang tersimpan pada Penyelenggara IIV	a	Jika Penyelenggara IIV bertukar informasi yang perlu dilindungi dengan organisasi lain, maka Penyelenggara IIV perlu meminta organisasi lain tersebut untuk menyetujui persyaratan keamanan untuk perlindungan informasi tersebut.	Tata Kelola
						b	Mengenkripsi informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan.	Teknologi
				2.3.2	Pelindungan terhadap data yang terkirim dari Penyelenggara IIV	a	Penyelenggara IIV memastikan saluran komunikasi menerapkan enkripsi saat berkomunikasi antara perangkat IIV dan server IIV.	Teknologi
						b	Penyelenggara IIV memastikan kunci enkripsi dikontrol dengan aman	Teknologi

							sepanjang siklus hidup kunci enkripsi tersebut untuk memastikan pengoperasian yang benar dan data yang ditransmisikan, diterima, dan disimpan dengan aman.	
				2.3.3	Memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai	a	Penyelenggara IIV menyediakan sumber daya yang cukup untuk setiap sistem IIV (misalnya ruang penyimpanan, sumber daya, dan sistem redundan),	Teknologi
						b	Penyelenggara IIV memastikan dilakukannya pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data.	Teknologi
				2.3.4	Mengimplementasikan pelindungan dari kebocoran data	a	Saat menangani informasi yang akan dilindungi atau pengadaan perangkat yang memiliki fungsi penting bagi organisasi, pilih perangkat dan server yang dilengkapi dengan perangkat *anti-tampering.*	Teknologi
						b	Memastikan bahwa jalur komunikasi yang digunakan untuk mengirim informasi telah dilindungi dengan kontrol keamanan yang tepat.	Teknologi
				2.3.5	Mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat	a	Melakukan pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan server pada waktu yang ditentukan oleh organisasi, untuk mencegah pemasangan perangkat lunak yang tidak sah.	Teknologi

					keras, dan data			
						b	Lakukan pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan.	Teknologi
						c	Memperkenalkan mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras.	Teknologi
						d	Konfirmasikan bahwa perangkat keras dan perangkat lunak adalah produk asli dan memiliki sertifikat keamanan.	Teknologi
						e	Pelihara, perbarui, dan kelola informasi seperti asal data, dan riwayat pemrosesan data, di seluruh siklus hidup data.	Tata Kelola & Teknologi
				2.3.6	Memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala	a	Tersedianya dan diterapkannya prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem.	Tata Kelola
				2.3.7	Menyediakan kebijakan pemusnahan data	a	Saat akan menghapuskan perangkat dan aset informasi, prosedur penghapusan data yang disimpan dari perangkat dan server serta informasi penting lainya (misalnya, kunci pribadi dan sertifikat digital), atau dibuat agar tidak dapat dibaca.	Tata Kelola
		2.4	Melindungi aplikasi	2.4.1	Menyediakan prosedur konfigurasi dasar	a	Tersedianya dan diterapkannya prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan	Tata Kelola

					sistem dan kendali perubahan konfigurasi		kata sandi, prosedur penerapan izin akses, dsb)	
						b	tersedianya dan diterapkanya prosedur untuk melakukan perubahan pengaturan pada perangkat.	Teknologi
						c	Tersedianya dan diterapkannya prosedur Pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan server.	Teknologi
				2.4.2	Mengembangkan dan mengimplementasikan rencana manajemen kerentanan.	a	Penyelenggara IIV mengembangkan dan mengimplementasikan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi.	Teknologi
				2.4.3	Memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional	a	Penggunaan lingkungan pengembangan sistem yang berbeda dari lingkungan produksi yang meliputi pemisahan terhadap media penyimpanan, jaringan, lingkungan kerja, dsb.	Tata Kelola
				2.4.4	Mengimplementasikan prosedur pengembangan sistem yang aman	a	tersedianya dan diterapkannya prosedur pengembangan perangkat lunak yang selalu memperhatikan aspek keamanan pada setiap tahapan siklus hidup pengembangannya.	Tata kelola dan teknologi

		2.5	Melindungi jaringan	2.5.1	Menerapkan sistem yang dikonfigurasi dengan prinsip fungsionalitas minimum	a	Minimalkan fungsi perangkat dan server dengan memblokir secara fisik dan logis port jaringan, USB, dan port serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan server.	Teknologi
						b	Memastikan Removable Media terlindungi dan penggunaannya terbatas sesuai dengan kebijakan.	Teknologi
				2.5.2	Menerapkan pelindungan terhadap jaringan komunikasi, akses sistem informasi, dan akses sistem kendali	a	Organisasi menentukan dan menerapkan segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet. (misalnya dibagi menjadi lingkungan pengembangan, pengujian, lingkungan produksi, dan lingkungan lain dalam organisasi)	Teknologi
						b	Jika diperlukan, organisasi juga dapat melakukan isolasi terhadap jaringan yang menghubungkan dengan perangkat penting, misalnya perangkat SCADA atau ICS (*Industrial Control System*).	Teknologi
				2.5.3	Menggunakan perangkat-perangkat jaringan yang menerapkan fungsi keamanan	a	Memastikan perangkat jaringan mampu menerapkan mekanisme (misalnya, *fail safe, load balancer, atau hot swap)* yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan.	Teknologi

						b	Memastikan fungsi keamanan pada perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan.	Teknologi
				2.5.4	Memastikan integritas jaringan senantiasa dilindungi	a	tersedianya prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai.	Teknologi
				2.5.5	Menerapkan prosedur dan teknologi pencegahan *malware*	a	Untuk melindungi ketersediaan data terhadap serangan malware, data organisasi harus di-rekam cadang secara berkala.	Teknologi
						b	pemindaian/*scanning* terhadap removable media yang akan digunakan pada perangkat komputer, *notebook*, *server*, atau perangkat pengolah informasi lainnya untuk mencegah masuknya virus dari luar ke dalam perangkat pengolah informasi dan jaringan komunikasi data milik Organisasi.	Teknologi
						c	Mengunduh dan menginstalasi update anti *malware* terbaru, meliputi *antivirus, anti-spyware, spam filtering, web content filtering, dan intrusion detection and prevention system.*	Teknologi
						d	Meng-update perangkat komputer dengan melakukan *upgrade* dan *patch* sistem operasi dan aplikasi.	Teknologi

				2.5.6	Memastikan catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan organisasi	a	Menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan log, dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar.	Tata Kelola
				2.5.7	Memastikan bahwa informasi mengenai pelindungan terhadap teknologi dibagikan hanya kepada pihak tepecaya	a	Berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya.	Tata Kelola
		2.6	Melindungi sumber daya manusia	2.6.1	Menerapkan prosedur pengelolaan keamanan terhadap personel	a	Pemeriksaan verifikasi latar belakang terhadap semua calon personel harus dilakukan sebelum bergabung dengan Penyelenggara IIV dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan.	Sumber Daya Manusia
						b	Perjanjian kontrak kerja harus menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.	Sumber Daya Manusia
						c	Proses pendisiplinan harus diformalkan dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan lainnya yang telah	Organisasi & Sumber Daya Manusia

							melakukan pelanggaran kebijakan keamanan informasi.	
						d	Organisasi menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi.	Sumber Daya Manusia
						e	Perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya.	Sumber Daya Manusia
						f	Langkah-langkah keamanan harus diterapkan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi.	Sumber Daya Manusia
						g	Organisasi harus menyediakan mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.	Sumber Daya Manusia
				2.6.2	Menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber	a	Memberikan pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi dan mengelola catatan sehingga mereka dapat memenuhi peran dan tanggung jawab yang ditugaskan untuk mencegah dan mengatasi	Sumber Daya Manusia

							terjadinya dan tingkat keparahan insiden keamanan.	
						b	Memberikan pelatihan dan pendidikan keamanan yang sesuai kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan. Kemudian, kelola catatan pelatihan dan pendidikan keamanan tersebut.	Sumber Daya Manusia
						c	Memberikan pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi dan mengelola catatan sehingga mereka dapat memenuhi peran dan tanggung jawab yang ditugaskan untuk mencegah dan mengatasi terjadinya dan tingkat keparahan insiden keamanan.	Sumber Daya Manusia
						d	Meningkatkan isi pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan organisasi.	Sumber Daya Manusia
				2.6.3	Menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di	a	Organisasi perlu menetapkan kebijakan terkait Kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya dengan menacu kepada Peta Okupasi Keamanan Siber Nasional Indonesia.	Sumber Daya Manusia

					Penyelenggara IIV	b	Organisasi perlu menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/workshop.	Sumber Daya Manusia
						c	Organisasi sektor Pemerintah harus meningkatkan keterampilan dan kompetensi teknis dalam keamanan siber serta perilaku personel terhadap keamanan siber secara berkala dan sesuai dengan perkembangan teknologi dan pemanfaatan TIK.	Sumber Daya Manusia
3	Deteksi	3.1	Mengelola deteksi Peristiwa Siber	3.1.1	Menetapkan peran dan tanggung jawab organisasi pada kebijakan pendeteksian Peristiwa Siber	a	Memperjelas peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan.	Tata Kelola
						b	Penyelenggara IIV menyiapkan sistem dalam organisasi untuk mendeteksi, menganalisis, dan merespons peristiwa keamanan.	Teknologi
				3.1.2	Melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku	a	Melakukan proses pemantauan peristiwa keamanan siber, sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku.	teknologi
						b	Melakukan pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi.	teknologi

				3.1.3	Menguji prosedur pendeteksian Peristiwa Siber secara berkala	a	Penyelenggara IIV melakukan pengujian secara periodik tentang efektifitas perangkat dan prosedur untuk mendeteksi peristiwa keamanan sebagaimana mestinya.	teknologi
				3.1.4	Menyampaikan informasi hasil pendeteksian Peristiwa Siber kepada pihak yang berhak	a	Informasi hasil pendeteksian kejadian keamanan diberitahukan kepada pihak yang terkait sesuai dengan persetujuan manajemen organisasi.	Tata Kelola
						b	Penyelenggara IIV melakukan reviu dan peningkatan prosedur pendeteksian peristiwa keamanan secara berkala.	Tata kelola
		3.2	Menganalisis anomali dan Peristiwa Siber	3.2.1	Menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data.	a	Penyelenggara IIV menetapkan dan menerapkan prosedur untuk mengidentifikasi dan mengelola ambang batas terhadap operasional jaringan dan arus informasi yang diharapkan antara pengguna, penyelenggara, dan sistem.	Tata Kelola
				3.2.2	Melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi	a	Kejadian keamanan yang terdeteksi dianalisis untuk memahami target dan metode serangan	Teknologi
						b	Identifikasi peristiwa keamanan secara akurat dengan menerapkan prosedur untuk melakukan analisis korelasi insiden keamanan dan analisis	Teknologi

							komparatif dengan informasi ancaman yang diperoleh dari luar organisasi.	
				3.2.3	Menentukan dampak dari Peristiwa Siber yang terdeteksi	a	Identifikasi dampak peristiwa keamanan, termasuk dampaknya terhadap organisasi lain yang relevan.	Teknologi
				3.2.4	Mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi	a	Hasil analisis peristiwa siber didokumentasikan, serta dilaporkan kepada pihak manajemen sesuai ketentuan.	Tata kelola
		3.3.	Memantau Peristiwa Siber berkelanjutan	3.3.1	Menerapkan prosedur pendeteksi kode berbahaya dan tak berizin	a	gunakan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan. (misalnya perangkat intrustion detection and prevention systems, next-generation firewall, endpoint detection and response, dll)	Teknologi
						b	memvalidasi apakah informasi atau file yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan.	Teknologi
						c	memvalidasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan.	Teknologi
				3.3.2	Memonitor kegiatan personel yang berada di dalam lingkup sistem IIV	a	Memastikan bahwa personel yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.	Sumber Daya Manusia

				3.3.3	Memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV	a	Memastikan bahwa pihak ketiga yang berada pada layanan IIV tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem IIV.	Tata kelola
				3.3.5	Menerapkan teknologi pemindaian kerentanan terhadap sistem IIV	a	Memastikan bahwa seluruh perangkat teknologi pada lingkup IIV telah diuji keamanannya melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.	Teknologi
						b	Penyelenggara IIV memastikan adanya pemeriksaan rutin di perangkat dan server yang dikelola dalam organisasi.	teknologi
4	Penanggulangan dan pemulihan	4.1	Menyusun perencanaan penanggulangan dan pemulihan insiden siber	4.1.1	Menyusun dan menetapkan rencana tanggap insiden siber yang disetujui oleh pimpinan organisasi	a	Menentukan dan menetapkan prosedur tanggap insiden beserta pembagian peran yang jelas antara pihak manajemen, personel pengelola IIV, dan pihak lainnya. yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya insiden siber.	Tata Kelola
						b	Menyusun dan menetapkan prosedur rencana tanggap insiden siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan	Tata Kelola
						c	Menentukan skenario insiden keamanan yang mungkin terjadi pada layanan IIV dan menambahkannya pada dokumen rencana tanggap insiden siber.	Tata Kelola

						d	Memastikan rencana tanggap insiden siber dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Tata Kelola
				4.1.2	Menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi	a	Menentukan dan menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan IIV, beserta daftar pembagian peran dan tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan IIV.	Tata Kelola
						b	Menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal.	Tata Kelola
						c	Menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital.	Tata Kelola
						d	Memastikan rencana keberlangsungan layanan dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Tata Kelola

				4.1.3	Memastikan rencana tanggap insiden siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala	a	Memastikan rencana tanggap insiden siber dan rencana keberlangsungan kegiatan disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup IIV. (misalnya dalam kegiatan simulasi kesiapsiagaan insiden siber)	Tata Kelola
				4.1.4	Memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap insiden siber dan rencana keberlangsungan kegiatan	a	Penyelenggara IIV menentukan dan menetapkan personel yang ditugaskan dalam tim tanggap insiden siber.	SDM & Tata Kelola
						b	Penyelenggara IIV memastikan personel mengetahui perannya dan urutan pengoperasian bila respons diperlukan	SDM & Tata Kelola
						c	Penyelenggara IIV mengidentifikasi siapa saja pihak-pihak pihak-pihak terkait dalam proses penanggulangan dan pemulihan insiden, misalnya aparat penegak hukum, regulator, maupun tim TTIS nasional	SDM & Tata Kelola
						d	Penyelenggara IIV perlu mengembangkan dan mengelola aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan. sehingga informasi organisasi hanya boleh keluar melalui personel yang berwenang saja.	SDM & Tata Kelola

				4.1.5	Memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang.	a	Penyelenggara IIV memastikan personel yang mengelola IIV melakukan prosedur rekam cadang untuk mengamankan aset informasi berupa sistem/data yang tersimpan di dalam sistem IIV, serta memastikan bahwa media yang digunakan untuk menyimpan data tersebut telah diamankan.	Tata Kelola
		4.2	Menganalisis dan melaporkan insiden siber	4.2.1	Mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal maupun sumber informasi eksternal	a	Penyelenggara IIV memastikan hasil analisis deteksi peristiwa siber diperiksa untuk menilai ada atau tidaknya anomali pada sistem.	teknologi
						b	Penyelenggara IIV mengumpulkan dan menganalisis laporan peristiwa siber yang diterima baik dari pengguna layanan, maupun sumber eksternal organisasi misalnya laporan dari Tim Tanggap Insiden Siber nasional atau mitra pihak ketiga.	teknologi
				4.2.2	Mengidentifikasi dan menganalisis potensi dampak dari insiden siber	a	Penyelenggara IIV harus mengidentifikasi dan menganalisis potensi dampak insiden siber pada layanan IIV, termasuk organisasi, dan pihak terkait seperti mitra ketiga berdasarkan laporan lengkap insiden siber.	teknologi
				4.2.3	Memastikan insiden siber dikategorikan sesuai kriteria yang telah ditetapkan	a	Penyelenggara IIV memastikan laporan insiden siber dikumpulkan, dikategorisasikan, dan diprioritaskan sesuai dampak risiko terhadap organisasi	Tata kelola

				4.2.4	Memastikan bahwa insiden siber dilaporkan kepada pihak yang terkait	a	Penyelenggara IIV memastikan informasi mengenai insiden siber dilaporkan kepada pihak yang berwenang sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku.	Tata Kelola
						b	Penyelenggara IIV memastikan proses koordinasi dengan para pemangku kepentingan dilakukan sesuai dengan rencana tanggap insiden siber (seperti kepada Kementerian atau Lembaga pembina sektor, Tim Tanggap Insiden Siber nasional, atau mitra pihak ketiga)	Tata Kelola
		4.3	Melaksanakan penanggulangan dan pemulihan insiden siber	4.3.1	Memastikan insiden siber diisolasi dan dimitigasi sesuai rencana tanggap insiden siber	a	Penyelenggara IIV harus mengambil langkah-langkah yang diperlukan untuk meminimalkan kerusakan terkait keamanan dan mengurangi dampak yang disebabkan oleh insiden tersebut. Misalnya melakukan isolasi terhadap jaringan yang terdapat insiden siber.	Tata Kelola
						b	Penyelenggara IIV harus mengidentifikasi hal-hal yang perlu diprioritaskan dan ruang lingkup respons yang perlu diambil.	Tata Kelola
						c	Penyelenggara IIV harus mengambil tindakan yang tepat terhadap perangkat yang terpengaruh oleh insiden siber, terutama mengenai fasilitas produksi yang rusak akibat insiden keamanan.	Tata Kelola
						d	Penyelenggara IIV mendokumentasikan hasil mitigasi insiden siber tersebut	Tata Kelola

							sebagai bahan pembelajaran berkelanjutan.	
				4.3.2	Mengumpulkan dan memelihara bukti insiden siber dari IIV terdampak	a	Penyelenggara IIV memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan.	Tata kelola
				4.3.3	Menginvestigasi dan eradikasi penyebab insiden siber	a	Untuk keperluan investigasi dan/atau audit, maka Penyelenggara IIV menerapkan forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukenali penyebab insiden.	Tata Kelola & teknologi
						b	Penyelenggara IIV harus memastikan bahwa seluruh aset informasi yang terdampak insiden siber telah diperiksa setiap komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait insiden siber	teknologi
				4.3.4	Mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan insiden siber	a	jika insiden meningkat atau meluas, maka Penyelenggara IIV perlu menyiapkan dan melaksanakan prosedur eskalasi insiden siber, seperti melaporkan kepada tim tanggap insiden siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait insiden	Tata Kelola

							siber tersebut.	
				4.3.5	Memastikan setiap aset informasi diperiksa keamanannya setelah penanganan insiden siber	a	Penyelenggara IIV melakukan pemeriksaan kepada seluruh aset informasi yang berhubungan dengan IIV untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi	teknologi
				4.3.6	Melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan	a	Penyelenggara IIV melaksanakan prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat.	teknologi
						b	Penyelenggara IIV melaksanakan simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik.	teknologi
						c	prosedur rekam cadang (*back-up*) sedapat mungkin dilakukan secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur *job-schedulling*.	Teknologi
						d	Penyelenggara IIV memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi.	Teknologi
						e	Penyelenggara IIV menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi.	Tata Kelola & Teknologi

						f	Penyelenggara IIV memastikan hasil pelaksanaan rekam cadang data didokumentasikan.	Tata Kelola & Teknologi
				4.3.7	Menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan	a	Penyelenggara IIV memastikan media penyimpanan rekam cadang telah disimpan secara aman.	Tata kelola
						b	pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi.	Tata Kelola
						c	pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi.	Teknologi
				4.3.8	Pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi.	a	Penyelenggara IIV harus menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan IIV telah beroperasi dengan normal pasca insiden siber	Tata Kelola
				4.3.9	Memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi insiden siber dan setelah penanggulangan serta pemulihan insiden siber	a	Penyelenggara IIV perlu menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber.	Tata Kelola
						b	Penyelenggara IIV memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan.	Tata Kelola

				4.3.10	Penyampaian informasi penanggulangan dan pemulihan insiden siber kepada pihak terkait	a	Penyelenggara IIV menyusun laporan hasil penanganan insiden siber dan menyampaikannya kepada Kementerian atau Lembaga di masing-masing sektor.	Tata kelola
		4.4	Meningkatkan keamanan setelah terjadinya insiden siber	4.4.1	Meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan	a	Penyelenggara IIV mengevaluasi kontrol keamanan yang diterapkan apakah masih relevan terhadap spektrum ancaman yang ada atau perlu ada perbaikan dan penambahan.	Tata Kelola
				4.4.2	Mereviu dan/atau memperbarui dokumen rencana tanggap insiden siber dan rencana keberlangsungan kegiatan secara berkala	a	Penyelenggara IIV melakukan reviu dan pembaharuan terhadap dokumen rencana tanggap insiden siber dan pemulihan jika terdapat hal-hal yang dapat dijadikan pembelajaran berkelanjutan bagi organisasi.	Tata Kelola
						b	Penyelenggara IIV mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko	Tata Kelola
				4.4.3	Mengumpulkan dan memelihara hasil forensik digital	a	Laporan hasil pelaksanaan forensik digital dikumpulkan dan dipelihara meliputi juga informasi-informasi yang relevan terhadapnya.	Tata kelola
						b	Laporan hasil pelaksanaan forensik digital dapat disampaikan kepada pihak berwajib untuk proses investigasi dan penegakkan hukum sesuai ketentuan yang berlaku	Tata kelola

				4.4.4	Meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap insiden siber secara berkala	a	Penyelenggara IIV melakukan peninjauan terhadap efektifitas kinerja penanganan insiden yang dilakukan oleh tim tanggap insiden siber secara berkala.	Tata Kelola
						b	Melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan insiden siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasistas SDM.	Tata Kelola

B. CONTOH FORMAT PENYUSUNAN PETA JALAN PELINDUNGAN IIV

PETA JALAN PELINDUNGAN IIV
(NAMA SEKTOR IIV)

I. Gambaran Umum
   a. Pendahuluan
   b. Tujuan
   c. Ruang Lingkup
II. Analisis Lingkungan Strategis Penyelenggaraan Pelindungan IIV (nama sektor IIV)
   a. Karakteristik layanan vital di sektor IIV (nama sektor)
   b. Analisis dampak yang di sektor (nama sektor)
   c. Regulasi nasional atau internasional pada sektor IIV (nama sektor)
   d. Analisis kondisi saat ini penerapan pelindungan pada sektor IIV (nama sektor)
   e. Analisis kesenjangan kondisi penerapan kontrol keamanan.
III. Rencana Peta Jalan Pelindungan IIV pada sektor (nama Sektor)
   a. Deskripsi arah kebijakan pelindungan IIV pada sektor (nama sektor)
   b. Deskripsi sasaran penyelenggaraan pelindungan IIV pada sektor (nama sektor)
   c. Deskripsi target penerapan Kontrol Keamanan
   d. Deskripsi rencana kerja penyelenggaraan pelindungan IIV
IV. Penutup

Tabel 2. Contoh Matriks Rencana Peta Jalan Pelindungan IIV pada Sektor (Nama Sektor)

Arah Kebijakan	**Sasaran Penyelenggaraan**	**Target Penerapan**	**Rencana Kerja**	**Waktu Pencapaian (*)**	**Pihak yang terlibat (*)**
Peningkatan/ pemenuhan kemampuan sektor *(nama sektor)* dalam mengidentifikasi konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV	Penyelenggara IIV pada sektor *(nama sektor)* mampu mengidentifikasi Peran dan tanggung Jawab Pelindungan IIV	seluruh Penyelenggara IIV pada sektor *(nama sektor)* telah mencapai Level 5	Penyusunan dan penetapan kebijakan yang berisi komitmen dan prioritas pimpinan organisasi terkait keamanan siber dan pelindungan IIV disetiap Penyelenggara IIV.	2024-2029	- Penyelenggara IIV
			Asistensi Penyusunan dan penetapan kebijakan keamanan siber disetiap Penyelenggara IIV	2024	- Kementerian atau Lembaga sektor IIV
	Dst..	Dst..	Dst..	Dst..	Dst..
Peningkatan/ pemenuhan kemampuan sektor (*nama sektor)* dalam mencegah, membatasi, atau menahan dampak dari ancaman dan/atau insiden siber.	Penyelenggara IIV pada sektor *(nama sektor)* mampu mengelola identitas, autentikasi, dan kendali akses pada layanan IIV	seluruh Penyelenggara IIV pada sektor *(nama sektor)* telah mencapai Level 5	Penyusunan pedoman pengelolaan terhadap identitas dan kredensial terhadap layanan IIV yang ada pada sektor *(nama sektor)*	2024	- Kementerian atau Lembaga sektor IIV - BSSN
			Melakukan penguatan pada proses pengelolaan identitias dan kredensial pada layanan IIV	2024-2028	- Penyelenggara IIV
	Dst..	Dst..	Dst..	Dst..	Dst..
Peningkatan/ pemenuhan kemampuan sektor (*nama sektor)*	Penyelenggara IIV pada sektor *(nama sektor)* mampu mengelola deteksi	seluruh Penyelenggara IIV pada sektor *(nama sektor)*	Penyusunan pedoman pedeteksian peristiwa siber pada layanan IIV di sektor *(nama sektor)*	2024	- Kementerian atau Lembaga sektor IIV - BSSN

dalam memantau secara tepat waktu terjadinya Peristiwa Siber	peristiwa siber pada layanan IIV	telah mencapai Level 4			
			Melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku	2024-2028	- Penyelenggara IIV
	Dst..	Dst..	Dst..	Dst..	Dst..
Peningkatan/ pemenuhan kemampuan sektor (*nama sektor)* dalam mengambil tindakan terkait penanggulangan dan pemulihan insiden siber	Penyelenggara IIV pada sektor *(nama sektor)* mampu menyusun perencanaan penanggulangan dan pemulihan insiden siber	seluruh Penyelenggara IIV pada sektor *(nama sektor)* telah mencapai Level 4	Penyusunan dan penetapan rencana tanggap insiden siber untuk setiap layanan IIV di Penyelenggara IIV	2025	- Penyelenggara IIV
			Mengembangkan rencana tanggap insiden siber sektoral	2024-2025	- Kementerian atau Lembaga sektor IIV - BSSN
Dst..	Dst..	Dst..	Dst..	Dst..	Dst..

*** :** waktu pencapaian, dan pihak yang terlibat ditentukan lebih lanjut oleh Kementerian atau Lembaga selaku instansi pengatur dan pengawas sektor IIV.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN