PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 5 TAHUN 2025
TENTANG
PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR ADMINISTRASI PEMERINTAHAN TAHUN 2025-2029

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang :

a. bahwa sektor administrasi pemerintahan telah ditetapkan sebagai salah satu sektor infrastruktur informasi vital;
b. bahwa untuk mengefektifkan penyelenggaraan pelindungan infrastruktur informasi vital sektor administrasi pemerintahan, diperlukan adanya peta jalan guna memberi arah dan langkah perencanaan serta pelaksanaan bagi penyelenggara infrastruktur informasi vital sektor administrasi pemerintahan;
c. bahwa berdasarkan ketentuan Pasal 8 ayat (1) Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Badan Siber dan Sandi Negara menyusun dan menetapkan peta jalan pelindungan infrastruktur informasi vital sebagaimana dimaksud dalam huruf b;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Peta Jalan Pelindungan Infrastruktur Informasi Vital Sektor Administrasi Pemerintahan Tahun 2025–2029;

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 Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

4. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital (Berita Negara Republik Indonesia Tahun 2023 Nomor 873);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR ADMINISTRASI PEMERINTAHAN TAHUN 2025-2029.

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. 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.
2. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
3. Penyelenggara IIV sektor administrasi pemerintahan yang selanjutnya disebut Penyelenggara IIV adalah instansi penyelenggara negara, badan usaha, dan/atau organisasi yang memiliki dan/atau mengoperasikan IIV dalam lingkup sektor administrasi pemerintahan.
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. Keamanan Siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik bersifat teknis maupun sosial.
8. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
9. Instansi Penyelenggara Negara adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan.
10. Kementerian atau Lembaga adalah Instansi Penyelenggara

Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya.

11. Badan Siber dan Sandi Negara yang selanjutnya disebut Badan adalah lembaga pemerintah yang melaksanakan tugas pemerintahan di bidang Keamanan Siber dan sandi.

Pasal 2

(1) Peta jalan pelindungan IIV sektor administrasi pemerintahan memuat:
   a. gambaran umum;
   b. analisis lingkungan strategis;
   c. matriks peta jalan; dan
   d. penutup

(2) Matriks peta jalan sebagaimana dimaksud pada ayat (1) huruf c terdiri atas:
   a. arah kebijakan;
   b. sasaran penyelenggaraan;
   c. target penerapan Kontrol Keamanan;
   d. rencana kerja; dan
   e. target dan tahun pencapaian

(3) Peta jalan pelindungan IIV sektor administrasi pemerintahan sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

(4) Peta jalan pelindungan IIV sektor administrasi pemerintahan sebagaimana dimaksud pada ayat (3) berlaku dari tahun 2025 sampai dengan tahun 2029

Pasal 3

(1) Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan melakukan reviu terhadap peta jalan pelindungan IIV sektor administrasi pemerintahan sebagaimana dimaksud dalam Pasal 2 setiap tahun.

(2) Dalam hal berdasarkan hasil reviu sebagaimana dimaksud pada ayat (1) diperlukan perubahan peta jalan pelindungan IIV sektor administrasi pemerintahan, Kepala Badan menetapkan perubahan peta jalan pelindungan IIV sektor administrasi pemerintahan.

Pasal 4

(1) Penyelenggara IIV melaksanakan peta jalan pelindungan IIV sektor administrasi pemerintahan sebagaimana dimaksud dalam Pasal 2.

(2) Dalam melaksanakan peta jalan pelindungan IIV sektor administrasi pemerintahan sebagaimana dimaksud pada ayat (1), Penyelenggara IIV berkoordinasi dengan Badan selaku Kementerian atau Lembaga.

Pasal 5

(1) Badan selaku Kementerian atau Lembaga melakukan pembinaan dan pengawasan terhadap pelaksanaan peta jalan pelindungan IIV sektor administrasi pemerintahan sebagaimana dimaksud dalam Pasal 2.

(2) Pembinaan sebagaimana dimaksud pada ayat (1) meliputi kegiatan:

a. mengoordinasikan peningkatan kapasitas sumber daya manusia yang ada di sektor administrasi pemerintahan;
b. penyelenggaraan kegiatan simulasi tanggap Insiden Siber untuk lingkup sektor yang diikuti oleh seluruh penyelenggara IIV sektor administrasi pemerintahan;
c. penyelenggaraan forum analisis dan berbagi informasi Keamanan Siber dalam lingkup sektor administrasi pemerintahan;
d. koordinasi teknis penyelenggaraan pelindungan IIV dalam lingkup sektor administrasi pemerintahan; dan/atau
e. kegiatan lain yang dibutuhkan oleh Penyelenggara IIV di sektor administrasi pemerintahan.

(3) Pengawasan sebagaimana dimaksud pada ayat (1) meliputi kegiatan:
a. menerima dan memverifikasi laporan penerapan peta jalan pelindungan IIV sektor administrasi pemerintahan yang dilakukan oleh Penyelenggara IIV; dan
b. pemantauan dan evaluasi penerapan peta jalan pelindungan IIV sektor administrasi pemerintahan yang dilakukan oleh Penyelenggara IIV berdasarkan hasil pengukuran tingkat kematangan Keamanan Siber yang dilaporkan oleh Penyelenggara IIV.

Pasal 6

(1) Dalam melakukan pembinaan dan pengawasan sebagaimana yang dimaksud dalam Pasal 5, Badan menyusun rencana kerja.
(2) Badan dalam menyusun rencana kerja sebagaimana dimaksud pada ayat (1) dapat melibatkan pihak lain yang diperlukan.
(3) Rencana kerja sebagaimana dimaksud pada ayat (1) ditetapkan dengan keputusan Kepala Badan.

Pasal 7

Pendanaan pelaksanaan peta jalan pelindungan IIV sektor administrasi pemerintahan bersumber dari:
a. anggaran dan pendapatan belanja negara;
b. anggaran dan pendapatan belanja daerah; dan/atau
c. sumber lain yang sah dan tidak mengikat,
sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 8

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 17 Februari 2025

KEPALA BADAN SIBER DAN SANDI NEGARA,

Ditandatangani secara elektronik oleh:
KEPALA BADAN SIBER DAN SANDI NEGARA

Hinsa Siburian
Letnan Jenderal TNI (Purn)

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 19 Februari 2025

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

#KUMHAMPASTI

Ditandatangani secara elektronik oleh :

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2025 NOMOR 110

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 5 TAHUN 2025
TENTANG
PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR ADMINISTRASI PEMERINTAHAN TAHUN 2025-2029

PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR ADMINISTRASI PEMERINTAHAN TAHUN 2025-2029

I. GAMBARAN UMUM

A. Pendahuluan

Presiden telah menetapkan Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital sebagai kebijakan nasional yang bertujuan untuk:

1. melindungi keberlangsungan penyelenggaraan IIV secara aman, andal, dan tepercaya;
2. mencegah terjadinya gangguan, kerusakan, dan/atau kehancuran pada IIV akibat serangan siber, dan/atau ancaman/kerentanan lainnya; dan
3. meningkatkan kesiapan dalam menghadapi Insiden Siber dan mempercepat pemulihan dari dampak Insiden Siber.

Untuk mengimplementasikan Peraturan Presiden Nomor 82 Tahun 2022 dimaksud dan sebagai pedoman dalam penyelenggaraan pelindungan IIV, Kepala Badan telah menetapkan 5 (lima) Peraturan Badan yang meliputi:

1. Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital;
2. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital;
3. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi;
4. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber; dan
5. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber.

Berdasarkan ketentuan peraturan perundang-undangan sebagaimana tersebut diatas, Badan sebagai Kementerian atau Lembaga sektor administrasi pemerintahan bertugas untuk menyusun dan menetapkan peta jalan pelindungan IIV sektor administrasi pemerintahan untuk memberi arah dan langkah perencanaan serta pelaksanaan bagi Penyelenggara IIV sektor administrasi pemerintahan. Adapun peta jalan pelindungan IIV sektor administrasi pemerintahan tersebut disusun dengan mengacu pada Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital yang ruang lingkupnya mengatur mengenai penyelenggaraan pelindungan IIV, pembinaan dan pengawasan, dan teknologi pelindungan IIV.

B. Tujuan

Peta jalan pelindungan IIV sektor administrasi pemerintahan bertujuan untuk menjadi acuan bagi Penyelenggara IIV dalam penyelenggaraan pelindungan IIV sektor administrasi pemerintahan tahun 2025-2029.

C. Ruang Lingkup

Peta jalan pelindungan IIV sektor administrasi pemerintahan memuat:

1. gambaran umum;
2. analisis lingkungan strategis;
3. arah kebijakan;
4. sasaran penyelenggaraan;
5. target penerapan Kontrol Keamanan;
6. rencana kerja; dan
7. penutup.

II. ANALISIS LINGKUNGAN STRATEGIS PENYELENGGARAAN PELINDUNGAN IIV SEKTOR ADMINISTRASI PEMERINTAHAN

Analisis lingkungan strategis penyelenggaraan pelindungan IIV sektor administrasi pemerintahan dimaksudkan untuk memberi gambaran kondisi penerapan Kontrol Keamanan saat ini di sektor administrasi pemerintahan. Analisis lingkungan strategis penyelenggaraan pelindungan IIV dilaksanakan dengan kegiatan:

A. Karakteristik Layanan Vital di Sektor Administrasi Pemerintahan dan Sistem Elektronik yang Menunjang Layanan Tersebut

Layanan vital di sektor administrasi pemerintahan merupakan layanan yang secara proses bisnis diselenggarakan oleh Instansi Penyelenggara Negara. Adapun penentuan layanan vital dimaksud dilakukan dengan mempertimbangkan karakteristik sebagai berikut:

1. layanan administrasi pemerintahan melalui Sistem Elektronik yang diselenggarakan secara berbagi pakai oleh Instansi Penyelenggara Negara;
2. layanan publik melalui Sistem Elektronik yang diselenggarakan secara berbagi pakai oleh Instansi Penyelenggara Negara;
3. layanan yang diselenggarakan untuk menyimpan dan/atau mengelola data dan informasi yang harus terjaga kerahasiaannya, integritasnya, dan/atau terjamin ketersediaannya;
4. layanan yang diselenggarakan melalui Sistem Elektronik untuk menyimpan data kependudukan sesuai ketentuan perundang-undangan;
5. penyelenggaraan layanan yang bersifat penyedia tunggal atau posisi dominan;
6. penyelenggaraan layanan yang sebagian besar berbentuk jasa;
7. penyelenggaraan layanan yang berupa pemberian perizinan;
8. penyelenggaraan layanan yang memberikan manfaat besar bagi masyarakat minimal 200.000 (dua ratus ribu) pengguna dan/atau target pengguna;
9. penyelenggaraan layanan yang ditujukan tidak semata untuk mencari keuntungan; dan/atau
10. penyelenggaraan layanan berdasarkan amanat ketentuan peraturan perundang-undangan.

Karakteristik layanan vital pada sektor administrasi pemerintahan memiliki keterkaitan, baik antar sesama layanan di sektor administrasi pemerintahan maupun dengan sektor IIV lainnya. Sebagai contoh, gangguan terhadap IIV sektor administrasi pemerintahan terkait layanan kependudukan dapat berdampak serius, baik terhadap pelayanan publik lainnya pada sektor administrasi pemerintahan, maupun pelayanan publik pada sektor IIV lainnya, antara lain layanan finansial pada sektor keuangan.

Selain itu, penyelenggaraan layanan vital juga dapat melibatkan penyelenggara Sistem Elektronik lingkup privat yang menjadi bagian dari dukungan operasional layanan tersebut. Karena itu, aspek penyelenggaraan pelindungan IIV juga harus diterapkan pada infrastruktur milik atau yang dikelola penyelenggara Sistem Elektronik lingkup privat tersebut.

B. Analisis Dampak yang Mungkin Timbul dari Gangguan Terhadap Layanan Vital dan Sistem Elektronik yang Menunjang Layanan Tersebut

Penyelenggaraan layanan vital di sektor administrasi pemerintahan

menghadapi ancaman Keamanan Siber yang berdampak pada kerahasiaan, keutuhan, dan ketersediaan informasi elektronik dan/atau dokumen elektronik. Sumber ancaman tersebut dapat berasal dari internal dan/atau eksternal organisasi yang dapat menimbulkan risiko keamanan dan mengganggu pencapaian tujuan dalam menyelenggarakan layanan bagi masyarakat.

Merujuk pada laporan tahunan Hasil Monitoring Keamanan Siber Badan Siber dan Sandi Negara tahun 2024, bahwa terdapat 330.527.636 (tiga ratus tiga puluh juta lima ratus dua puluh tujuh ribu enam ratus tiga puluh enam) anomali serangan siber di Indonesia selama kurun waktu tahun 2024. Total anomali tersebut secara garis besar didominasi di sektor administrasi pemerintahan yang terindikasi sebanyak 30.442.122 (tiga puluh juta empat ratus empat puluh dua ribu seratus dua puluh dua) temuan data/informasi kredensial akun dari sistem informasi milik pemerintahan yang dipublikasi di *darknet*.

Metode yang digunakan adalah *passive monitoring* yang merupakan pencarian informasi dan monitoring terkait kerentanan/ *Common Vulnerabilities and Exposures* berdasarkan alamat protokol internet (*internet protocol)* dan domain milik Instansi Penyelenggara Negara pada sektor administrasi pemerintahan dengan menggunakan data yang tersedia melalui sumber terbuka. Notifikasi indikasi Insiden Siber yang telah diberikan Badan selama tahun 2024 menunjukkan sektor administrasi pemerintahan menjadi sektor penerima notifikasi terbanyak dengan kategori indikasi Insiden Siber berupa kebocoran data, anomali jaringan dan aktivitas jahat.

Indikasi kerentanan yang ditemukan pada sektor administrasi pemerintahan harus segera ditindaklanjuti untuk mencegah terjadinya eksploitasi yang menyebabkan terganggunya proses bisnis organisasi maupun pencurian dan/atau manipulasi data. Oleh karena itu, setiap ancaman keamanan pada layanan vital harus dapat dikelola dan dimitigasi melalui langkah strategis dan sistematis agar organisasi dapat terhindar dari beberapa ancaman yang akan berpotensi menimbulkan risiko terhadap pencapaian tujuan organisasi.

Dampak yang mungkin timbul dari gangguan terhadap penyelenggaraan IIV mempertimbangkan seluruh level dampak baik dari organisasi, intra sektor, antar sektor, maupun eskalasi sampai dengan level nasional. Gangguan, kegagalan, kerusakan, dan/atau kehancuran pada IIV diakibatkan oleh salah satu atau kombinasi dari kategori dampak yang meliputi:

1. dampak operasional adalah berbagai akibat yang ditimbulkan karena kegagalan, tidak memadainya prosedur, kesalahan orang, sistem, atau sumber eksternal yang memengaruhi kondisi atau keberlangsungan layanan baik dalam ruang lingkup instansi atau institusi, sektoral, dan berpotensi berdampak pada level nasional;
2. dampak terhadap data dan/atau informasi adalah berbagai akibat yang timbul akibat pengungkapan, modifikasi, gangguan akses, ketersediaan terhadap data, informasi, Sistem Elektronik yang menyimpan atau mengelola data dan/atau informasi yang memengaruhi kondisi, keberlangsungan layanan baik dalam lingkup instansi atau institusi, sektoral, dan berpotensi berdampak pada level nasional;
3. dampak finansial adalah berbagai akibat yang ditimbulkan karena kegagalan atau tidak memadainya prosedur, kesalahan orang, sistem dan/atau sumber eksternal sehingga mengakibatkan penundaan, kehilangan pendapatan, dan/atau arus kas suatu instansi atau institusi, yang memengaruhi kondisi, atau keberlangsungan layanan

baik dalam lingkup instansi atau institusi, sektoral, dan berpotensi berdampak pada level nasional;

4. dampak umum adalah berbagai akibat yang ditimbulkan karena kegagalan atau tidak memadainya prosedur, kesalahan orang, sistem atau sumber eksternal sehingga mengakibatkan gangguan dan/atau kegagalan terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan serta perekonomian nasional;
5. dampak saling ketergantungan adalah akibat yang ditimbulkan terhadap layanan, atau fungsi pada suatu instansi, institusi atau sektor, karena gangguan dan/atau kegagalan layanan atau fungsi pada instansi, institusi atau sektor lain yang memiliki hubungan saling ketergantungan layanan, dan/atau sistem satu sama lain.

Dampak terjadinya gangguan atau kegagalan penyelenggaraan IIV sektor administrasi pemerintahan mempertimbangkan pula durasi dari dampak tersebut yang terdiri atas:

1. Jangka pendek: menyebabkan hambatan dalam aktivitas masyarakat, penundaan proses, penjadwalan ulang aktivitas, kerugian materil dan aspek keamanan/keselamatan/kesehatan sebagian masyarakat.
2. Jangka menengah – panjang: perubahan dalam pola kehidupan masyarakat, kerugian materiil yang memerlukan waktu sumber daya besar untuk pemulihan atau perbaikannya sampai penurunan tingkat ketahanan nasional.

Pendekatan manajemen risiko keamanan dalam penyelenggaraan IIV harus memperhatikan dampak yang dapat terjadi, baik jangka pendek, maupun jangka menengah-panjang untuk memastikan upaya mitigasi dapat diterapkan secara efektif dan efisien.

C. Identifikasi Kegiatan Regulasi Nasional dan/atau Internasional yang Terkait Dalam Operasional Layanan Vital Tersebut

Terdapat beberapa Peraturan Perundang-undangan yang mengatur hal ihwal terkait penyelenggaraan pelindungan IIV sektor administrasi pemerintahan, antara lain:

1. Undang-undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (UU Pemda)

   UU Pemda mengatur mengenai pembagian urusan pemerintahan antara pemerintah pusat, pemerintah daerah provinsi, dan pemerintah daerah kabupaten/kota. Penyelenggaraan layanan di pemerintah daerah diarahkan untuk mempercepat terwujudnya kesejahteraan masyarakat melalui peningkatan pelayanan, pemberdayaan, dan peran serta masyarakat, serta peningkatan daya saing daerah. Dalam rangka mendukung kelancaran fungsi pemerintahan dan pelayanan publik, pemerintah daerah menggunakan Sistem Elektronik dengan memanfaatkan teknologi informasi dan/atau teknologi operasional yang berperan sangat penting dalam proses bisnis penyelenggaraan pemerintahan daerah.

   Pada konteks pelindungan IIV sektor administrasi pemerintahan pada pemerintah daerah, dapat dikaitkan dengan wewenang pemerintah daerah baik pengaturan urusan pemerintahan absolut maupun urusan pemerintahan konkuren. Urusan pemerintahan absolut merupakan wewenang pemerintah pusat dalam rangka penetapan, pembinaan, dan pengawasan pelaksanaan kebijakan pelindungan IIV secara nasional, sementara untuk implementasi kebijakan pelindungan IIV di daerah kiranya dapat menjadi urusan pemerintahan konkuren.

2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

   Peraturan Pemerintah Nomor 71 Tahun 2019 ditetapkan untuk mengatur secara menyeluruh pemanfaatan teknologi informasi dan transaksi elektronik di wilayah Indonesia. Dalam peraturan tersebut telah menetapkan bahwa Instansi Penyelenggara Negara dan institusi yang ditunjuk oleh Instansi Penyelenggara Negara merupakan penyelenggara Sistem Elektronik lingkup publik yang wajib menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Sektor administrasi pemerintahan merupakan salah satu sektor dalam penyelenggara Sistem Elektronik lingkup publik yang diwajibkan untuk melindungi data elektronik strategis atau yang mempunyai IIV.

   Penyelenggara Sistem Elektronik di sektor administrasi pemerintahan yang memiliki data elektronik strategis selanjutnya diharuskan membuat dokumen elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu untuk kepentingan pengamanan data. Ketentuan mengenai kewajiban membuat dokumen elektronik dan rekam cadang elektroniknya serta menghubungkannya ke pusat data tertentu tersebut dilaksanakan sesuai dengan peraturan perundang- undangan.

3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik

   Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik ditetapkan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan tepercaya dalam penyelenggaraan layanan berbasis digital yang dilaksanakan oleh penyelenggara Sistem Elektronik pada sektor administrasi pemerintahan serta untuk meningkatkan keterpaduan dan efisiensi Sistem Pemerintahan Berbasis Elektronik (SPBE). Penyelenggaraan SPBE mengacu pada arsitektur SPBE yang terdiri atas domain layanan, proses bisnis, data dan informasi, aplikasi, infrastruktur, dan keamanan.

   Dalam rangka menyelenggarakan layanan melalui SPBE, penyelenggara Sistem Elektronik pada sektor administrasi pemerintahan harus menerapkan Keamanan SPBE melalui pemenuhan standar teknis dan prosedur keamanan SPBE. Pemenuhan keamanan SPBE tersebut harus diterapkan pada aplikasi dan infrastruktur baik yang dikelola secara nasional maupun oleh masing-masing penyelenggara Sistem Elektronik di sektor administrasi pemerintahan.

4. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional

   Peraturan Presiden Nomor 132 Tahun 2022 mengatur mengenai arsitektur SPBE yang diterapkan secara nasional. Peraturan tersebut merupakan langkah strategis yang dilakukan oleh pemerintah Indonesia untuk memperkuat digitalisasi pada sektor administrasi pemerintahan. Tujuan disusunnya arsitektur SPBE nasional ini adalah untuk memberikan panduan dalam pelaksanaan integrasi proses bisnis, data dan informasi, aplikasi SPBE, infrastruktur SPBE, dan keamanan SPBE untuk menghasilkan operasional layanan pemerintah yang terpadu secara nasional. Selain itu, juga untuk mendeskripsikan integrasi proses bisnis, data dan informasi, aplikasi SPBE,

infrastruktur SPBE, dan keamanan SPBE untuk menghasilkan layanan pemerintah yang terintegrasi. Melalui peraturan tersebut, Presiden telah menetapkan pula layanan yang termasuk dalam inisiatif strategis.

Arsitektur SPBE nasional yang diatur dalam Peraturan Presiden Nomor 132 Tahun 2022 mencakup arah kebijakan dan strategi dalam penyusunan arsitektur SPBE nasional yang memperhatikan keselarasan program pembangunan nasional yang

didasarkan pada Rencana Pembangunan Jangka Menengah Nasional 2020-2024, pengarusutamaan transformasi digital, kebijakan satu data Indonesia, serta arah kebijakan dan strategi SPBE. Selain arah kebijakan dan strategi, peraturan tersebut mengatur juga kerangka kerja, referensi, domain, dan inisiatif strategis arsitektur SPBE nasional.

5. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber

   Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber ini ditetapkan guna untuk melindungi segenap bangsa dan kepentingan nasional dari penyalahgunaan sumber daya siber dan untuk mempersiapkan secara dini dalam menghadapi krisis siber dan memulihkan situasi dari krisis siber. Strategi Keamanan Siber nasional dan manajemen krisis siber merupakan acuan bagi Instansi Penyelenggara Negara dan pemangku kepentingan untuk mewujudkan kekuatan dan kapabilitas siber dalam rangka mencapai stabilitas Keamanan Siber.

   Penguatan pelindungan IIV merupakan salah satu fokus area strategi Keamanan Siber nasional yang diatur dalam Peraturan Presiden tersebut, yaitu meliputi penyelenggaraan pelindungan IIV dan peningkatan pembinaan dan pengawasan penyelenggaraan pelindungan IIV. Sektor administrasi pemerintahan memiliki peranan penting dalam pelindungan IIV karena mendukung terselenggaranya strategi Keamanan Siber secara nasional.

6. Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional

   Peraturan Presiden Nomor 82 Tahun 2023 tentang Percepatan Transformasi Digital dan Keterpaduan Layanan Digital Nasional bertujuan untuk mewujudkan pelayanan publik yang berkualitas dan tepercaya, SPBE dan satu data Indonesia yang terpadu dan menyeluruh, birokrasi dan pelayanan publik yang berkinerja tinggi, penguatan pencegahan korupsi, dan penguatan aspek Keamanan Siber dan keamanan informasi. Guna mewujudkan tujuan tersebut pemerintah melakukan percepatan transformasi digital melalui penyelenggaraan aplikasi SPBE prioritas dengan mengutamakan integrasi dan interoperabilitas.

   Aplikasi SPBE prioritas diselenggarakan untuk mendukung layanan pendidikan terintegrasi, kesehatan terintegrasi, bantuan sosial terintegrasi, administrasi kependudukan yang terintegrasi dengan layanan identitas kependudukan digital, layanan pembayaran terpadu yang terintegrasi, administrasi pemerintahan di bidang aparatur negara yang terintegrasi, portal pelayanan publik, satu data Indonesia, dan layanan kepolisian yang terintegrasi.

7. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik

   Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik

tersebut menjadi acuan dalam tahap pelaksanaan identifikasi IIV dan operasional layanan vital sektor administrasi pemerintahan. Sistem pengamanan dalam penyelengaraan Sistem Elektronik dilaksanakan melalui sistem manajemen pengamanan informasi yang dalam penerapannya berdasarkan pada asas risiko. Penyelenggara Sistem Elektronik sektor administrasi pemerintahan harus melakukan identifikasi IIV terhadap Sistem Elektronik yang dimiliki dan/atau dikelola dengan langkah awal menentukan kategori Sistem Elektronik sesuai ketentuan pada peraturan ini. Kategori Sistem Elektronik terdiri atas Sistem Elektronik dengan kategori strategis, tinggi, dan rendah. Sistem Elektronik dengan kategori strategis menjadi prioritas untuk dilakukan pengukuran tingkat vitalitas dari Sistem Elektronik yang dikelola.

8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik

   Pedoman manajemen keamanan informasi merupakan acuan Instansi Penyelenggara Negara dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan program kerja keamanan SPBE, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan. Serangkaian proses manajemen keamanan informasi tersebut harus ditetapkan oleh setiap pimpinan Instansi Penyelenggara Negara untuk selanjutnya digunakan sebagai pedoman pelaksanaan keamanan informasi dengan ruang lingkup organisasi. Oleh sebab itu, diharapkan penerapan keamanan tidak hanya sebatas pada ruang lingkup unit kerja atau layanan tertentu.

   Peraturan tersebut juga mengamanatkan agar seluruh Instansi Penyelenggara Negara menerapkan keamanan sesuai standar teknis dan prosedur keamanan yang terdiri atas keamanan data dan informasi, aplikasi baik yang berbasis *web* maupun *mobile,* sistem penghubung layanan, jaringan intra dan pusat data nasional.

9. Peraturan Badan Siber dan Sandi Negara Nomor 7 Tahun 2023 tentang Identifikasi Infrastruktur Informasi Vital

   Penyelenggara Sistem Elektronik memiliki kewajiban untuk melakukan identifikasi IIV secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun. Proses identifikasi IIV ini dilakukan untuk menilai sistem elektronik yang dikelola berdasarkan penentuan kategorisasi Sistem Elektronik dan pengukuran tingkat vitalitas Sistem Elektronik yang dikelola. Mekanisme dalam melakukan identifikasi IIV melibatkan dua pihak, yaitu penyelenggara Sistem Elektronik sebagai pelaksana penilaian mandiri pada Sistem Elektronik yang berpotensi menjadi IIV dan Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan sebagai verifikator atas laporan hasil penilaian mandiri.

   Identifikasi IIV ini merupakan prosedur yang mengikat dan menjadi tahap awal bagi penyelenggara Sistem Elektronik dalam mengimplementasikan penyelenggaraan IIV. Berdasarkan hasil verifikasi tersebut, maka Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan akan melakukan penetapan IIV dan Penyelenggara IIV bagi penyelenggara Sistem Elektronik yang telah terverifikasi mengoperasikan IIV.

10. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2023 tentang Kerangka Kerja Pelindungan Infrastruktur Informasi Vital

Peraturan ini ditetapkan untuk memberikan pedoman bagi Penyelenggara IIV dalam penyelenggaraan pelindungan IIV di organisasi masing-masing, termasuk sektor administrasi pemerintahan. Pengaturan kerangka kerja dijadikan acuan bagi Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan dalam menyusun serta menetapkan peta jalan pelindungan IIV di sektor administrasi pemerintahan.

Dalam penyelenggaraan pelindungan IIV, Penyelenggara IIV melaksanakan serangkaian upaya untuk mengendalikan keamanan melalui penerapan Kontrol Keamanan pada IIV sesuai dengan domain identifikasi, proteksi, deteksi, serta penanggulangan dan pemulihan. Pembinaan dan pengawasan penyelenggaraan pelindungan IIV dilakukan untuk memastikan berjalan sesuai dengan peta jalan pelindungan IIV di sektor administrasi pemerintahan. Penyelenggara IIV juga wajib memastikan keamanan perangkat teknologi pelindungan IIV yang digunakan dibuktikan dengan tanda sertifikasi. Tanda sertifikasi dilakukan verifikasi dan/atau rekognisi oleh Badan sesuai dengan ketentuan peraturan perundang-undangan.

11. Peraturan Badan Siber dan Sandi Negara Nomor 9 Tahun 2023 tentang Peningkatan Kapasitas Sumber Daya Manusia di Bidang Keamanan Siber dan Sandi

    Peningkatan kapasitas sumber daya manusia yang diatur dalam Peraturan ini meliputi penyediaan sumber daya manusia bidang Keamanan Siber dan sandi, peningkatan kompetensi, sertifikasi kompetensi, alih teknologi dan alih keahlian, dan peningkatan budaya kesadaran keamanan informasi. Penyelenggara IIV wajib melaksanakan peningkatan kapasitas sumber daya manusia paling sedikit melalui peningkatan kompetensi dan/atau sertifikasi kompetensi, alih teknologi dan alih keahlian, dan peningkatan budaya kesadaran keamanan informasi. Peningkatan kompetensi dilaksanakan dengan mengacu pada standar kompetensi bidang Keamanan Siber dan sandi yaitu Standar Kompetensi Kerja Nasional Indonesia (SKKNI) bidang Keamanan Siber, standar kompetensi jabatan bidang Keamanan Siber dan sandi, atau standar kompetensi bidang Keamanan Siber dan sandi lainnya.

    Sedangkan, untuk sertifikasi kompetensi diperoleh berdasarkan hasil uji kompetensi yang dilaksanakan oleh lembaga sertifikasi profesi yang telah teregister di Badan atau instansi pembina bagi sumber daya manusia bidang Keamanan Siber dan sandi untuk Aparatur Sipil Negara. Dalam hal alih teknologi dan alih keahlian, Penyelenggara IIV harus melaksanakannya sesuai dengan peraturan perundang-undangan yang berlaku.

12. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber

    Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber mengatur mengenai pelaksanaan, pelaporan, dan verifikasi pengukuran tingkat kematangan Keamanan Siber. Penyelenggara IIV paling sedikit melakukan pengukuran tingkat kematangan Keamanan Siber 1 (satu) kali dan 1 (satu) tahun secara mandiri berdasarkan domain pada kerangka kerja pelindungan IIV dan melaporkannya sesuai peraturan perundang-undangan.

    Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan melakukan verifikasi atas laporan hasil pengukuran tingkat kematangan Keamanan Siber dari Penyelenggara IIV. Hasil dari

verifikasi tersebut selanjutnya dilaporkan kepada Badan dan Penyelenggara IIV untuk diketahui level hasil penilaian atas kondisi yang menggambarkan kapabilitas dan kemajuan organisasi dalam menerapkan, meningkatkan, dan menjalankan Keamanan Siber secara efektif dan efisien. Hasil penilaian tersebut menjadi capaian target penerapan Kontrol Keamanan sesuai dengan peta jalan pelindungan IIV sektor administrasi pemerintahan.

13. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber

    Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 mencakup berbagai aspek pengaturan mulai dari pembentukan Tim Tanggap Insiden Siber hingga prosedur pelaporan dan penanganan Insiden Siber. Peraturan tersebut mengamanatkan pembentukan Tim Tanggap Insiden Siber di berbagai tingkat, yaitu nasional, sektoral, dan organisasi. Setiap Tim Tanggap Insiden Siber memiliki tugas spesifik dalam penanganan Insiden Siber di tingkat masing-masing. Setiap Penyelenggara IIV diwajibkan membentuk Tim Tanggap Insiden Siber untuk mengelola dan merespon Insiden Siber yang terjadi di lingkup organisasi mereka. Tugas Tim Tanggap Insiden Siber adalah memberikan peringatan, panduan teknis, serta melakukan koordinasi penanganan Insiden Siber.

    Penanganan Insiden Siber melibatkan langkah-langkah untuk menanggulangi, memulihkan, dan mendistribusikan informasi untuk mengurangi dampak dari insiden. Ini mencakup tindakan teknis dan administratif yang diperlukan untuk mengatasi ancaman siber. Dengan adanya Tim Tanggap Insiden Siber, diharapkan segala bentuk ancaman dan Insiden Siber dapat ditangani dengan cepat dan tepat, sehingga mengurangi risiko terhadap Keamanan Siber.

D. Identifikasi Kegiatan Pelindungan yang Telah Diterapkan pada Layanan Vital dari Aspek Ketersediaan dan Kemampuan Sumber Daya Manusia, Tata Kelola, dan Teknologi

Badan memiliki peran sebagai koordinator penyelenggaraan pelindungan IIV secara nasional sekaligus sebagai Kementerian atau Lembaga sektor administrasi pemerintahan dan juga sebagai penyelenggara Sistem Elektronik. Selaku Kementerian atau Lembaga sektor administrasi Badan telah melakukan pembinaan dan pengawasan dalam rangka penerapan pelindungan IIV sesuai dengan ketentuan dalam Peraturan Presiden Nomor 82 Tahun 2022 sebagai berikut:

1. Inventarisasi dan kategorisasi Sistem Elektronik pada sektor administrasi pemerintahan

   Badan sebagai Kementerian atau Lembaga sektor administrasi pemerintahan telah melakukan kegiatan inventarisasi dan kategorisasi Sistem Elektronik pada Instansi Penyelenggara Negara yang meliputi instansi pusat dan pemerintah daerah baik pemerintah provinsi maupun pemerintah kabupaten/kota. Berdasarkan kegiatan tersebut, diperoleh gambaran kondisi sektor administrasi pemerintahan sebagai berikut:
   a. Instansi Penyelenggara Negara belum melakukan inventarisasi aset dan kategorisasi Sistem Elektronik;
   b. Instansi Penyelenggara Negara sudah melakukan inventarisasi aset, tetapi belum melakukan kategorisasi Sistem Elektronik; atau
   c. Instansi Penyelenggara Negara sudah melakukan inventarisasi aset dan baru sebagian melakukan kategorisasi Sistem Elektronik.

2. Identifikasi dan penetapan IIV sektor administrasi pemerintahan

Dalam melakukan kegiatan identifikasi dan penetapan terhadap Sistem Elektronik menjadi IIV dan penyelenggara Sistem Elektronik sebagai Penyelenggara IIV, Badan sebagai Kementerian atau Lembaga sektor administrasi pemerintahan telah melakukan pengukuran tingkat vitalitas Sistem Elektronik sampai dengan melakukan penetapan IIV. Kondisi saat ini, sektor administrasi pemerintahan telah melakukan berbagai kegiatan untuk mendukung keperluan identifikasi IIV, yaitu:

a. *Focus Group Discussion* (FGD) identifikasi IIV sektor administrasi pemerintahan

   FGD bertujuan untuk memberikan gambaran dan diseminasi pelaksanaan identifikasi IIV, dasar hukum pelaksanaan pelindungan IIV, termasuk peraturan perundang- undangannya. Pada tahun 2024, FGD diikuti oleh 32 (tiga puluh dua) Instansi Penyelenggara Negara yang terdiri atas 22 (dua puluh dua) instansi pusat dan 10 (sepuluh) pemerintah daerah.

b. *Workshop* Identifikasi IIV sektor administrasi pemerintahan

   Workshop tahun 2024 diikuti oleh 40 (empat puluh) Instansi Penyelenggara Negara yang terdiri atas 30 (tiga puluh) instansi pusat dan 10 (sepuluh) pemerintah daerah yang bertujuan untuk memberikan gambaran, asistensi dan penjelasan tata cara pelaksanaan identifikasi IIV mulai dari melakukan inventarisasi aset, kategorisasi Sistem Elektronik, pengukuran vitalitas IIV, hingga penyusunan laporan identifikasi IIV.

c. Verifikasi dan penetapan IIV sektor administrasi pemerintahan Pada tahun 2024 telah dilakukan verifikasi terhadap 81 (delapan puluh satu) penyelenggara Sistem Elektronik yang berasal dari 25 (dua puluh lima) instansi pusat dan 10 (sepuluh) pemerintah daerah dengan total 128 (seratus dua puluh delapan) Sistem Elektronik. Berdasarkan hasil verifikasi, telah ditetapkan 36 (tiga puluh enam) Sistem Elektronik menjadi IIV sektor administrasi pemerintahan dan 1 (satu) Sistem Elektronik ditetapkan menjadi IIV sektor kesehatan. Sejumlah 36 (tiga puluh enam) IIV sektor administrasi pemerintahan tersebut berasal dari 27 (dua puluh tujuh) Penyelenggara IIV pada 19 (sembilan belas) instansi pusat.

3. Pengukuran tingkat kematangan Keamanan Siber di sektor administrasi pemerintahan

   Badan telah melakukan pengukuran tingkat kematangan Keamanan Siber dengan menggunakan instrumen *Cyber Security Maturity* (CSM) kepada Instansi Penyelenggara Negara, terakhir dilakukan pada tahun 2024. Hasil pengukuran instrumen CSM yang terdiri atas 5 (lima) domain yaitu tata kelola, identifikasi, proteksi, deteksi, dan respon akan diselaraskan dengan instrumen pengukuran tingkat kematangan Keamanan Siber yang diatur dalam Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2023 tentang Pengukuran Tingkat Kematangan Keamanan Siber.

4. Pelaksanaan kerja sama dalam negeri dan luar negeri dalam rangka penyelenggaraan pelindungan IIV

   Sektor administrasi pemerintahan telah menyelenggarakan kerja sama dengan instansi maupun praktisi untuk mendukung penyelenggaraan pelindungan IIV berupa pemberian masukkan terhadap peta jalan pelindungan IIV sektor administrasi pemerintahan serta kerangka kerja penerapan pelindungan IIV. Kerja sama luar negeri yang telah dilakukan adalah pertukaran praktik baik pelindungan IIV dan berbagi informasi Keamanan Siber dengan negara

Amerika Serikat, Australia, Arab Saudi, Tiongkok, Inggris Raya, Korea Selatan, Persatuan Emirat Arab, Rusia, Slowakia, dan Belanda. Untuk mendukung keberlanjutan kerja sama tersebut, perencanaan dan konsep kegiatan kerja sama dalam dan luar negeri untuk penyelenggaraan pelindungan IIV sector administrasi pemerintahan telah dituangkan dalam bentuk rencana kerja dan Rencana Pembangunan Jangka Menengah (RPJM) Tahun 2025-2029.

5. Pembentukan dan pelaksanaan fungsi Tim Tanggap Insiden Siber sektor administrasi pemerintahan

   Badan telah memiliki Tim Tanggap Insiden Siber Nasional atau *Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center* (ID-SIRTII) yang bertugas melakukan penanganan Insiden Siber pada tingkat nasional. Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan telah membentuk dan mengoperasionalkan Tim Tanggap Insiden Siber sektor administrasi pemerintahan yaitu Gov-CSIRT. Dalam pelaksanaannya, Gov-CSIRT maupun ID-SIRTII telah melakukan kegiatan operasional seperti layanan monitoring anomali jaringan, insiden respon, forensik digital, *cyber threat intelligent*, analisis *malware* dan penerapan *deception technology* (*honeynet*), *threat hunting* serta bentuk operasi gabungan/kolaborasi lainnya baik skala nasional maupun internasional.

6. Asistensi pembentukan Tim Tanggap Insiden Siber organisasi sektor administrasi pemerintahan

   Tim Tanggap Insiden Siber organisasi memiliki tugas dan fungsi penanganan Insiden Siber pada level organisasi. Penanganan Insiden Siber dilakukan dengan melalui penanggulangan dan pemulihan Insiden Siber, penyampaian informasi Insiden Siber kepada pihak terkait, dan diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

   Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan menyelenggarakan asistensi pembentukkan Tim Tanggap Insiden Siber organisasi pada Instansi Penyelenggara Negara baik instansi pusat maupun pemerintah daerah. Kegiatan asistensi dilakukan mulai dari persiapan, perencanaan, sampai dengan pendampingan peluncuran Tim Tanggap Insiden Siber organisasi. Dalam tahap perencanaan, instansi pusat maupun pemerintah daerah diberikan pemahaman dokumen kebutuhan pembentukkan serta pembekalan teknis kepada personel Tim Tanggap Insiden Siber dalam menjalankan tugas dan fungsinya.

7. Penyelenggaraan kegiatan simulasi kesiapsiagaan terhadap Insiden Siber di sektor administrasi pemerintahan

   Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan telah menyelenggarakan kegiatan simulasi kesiapsiagaan terhadap insiden siber dengan sasaran peserta instansi pusat dan pemerintah daerah dalam bentuk *workshop* atau permohonan asistensi/narasumber. Adapun kegiatan ini merupakan simulasi dalam bentuk prosedural dan teknis melalui pemberian penjelasan dan studi kasus dalam menangani Insiden Siber atau proses eskalasinya hingga menekankan pentingnya dokumentasi dan keterlibatan manajemen/pimpinan. Kegiatan ini dimaksudkan agar instansi pusat dan pemerintah daerah dapat secara mandiri melakukan tanggap Insiden Siber.

8. Penyelenggaraan forum analisis dan berbagi informasi Keamanan Siber sektor administrasi pemerintahan

Forum analisis dan berbagi informasi Keamanan Siber yang telah diselenggarakan secara rutin oleh Gov-CSIRT adalah dalam bentuk kegiatan *communication check* dengan melibatkan peserta dari Tim Tanggap Insiden Siber instansi pusat dan pemerintah pemerintah daerah. Dalam kegiatan tersebut dilakukan berbagi informasi terkini mengenai kondisi Keamanan Siber di sektor administrasi pemerintahan, pelajaran yang dapat diambil dari Insiden Siber yang terjadi di sektor administrasi pemerintahan, simulasi prosedur penanganan Insiden Siber, serta upaya peningkatan Keamanan Siber sektor administrasi pemerintahan. Selain sebagai forum analisis dan berbagi informasi, kegiatan *communication check* bertujuan untuk memperbarui narahubung setiap Tim Tanggap Insiden Siber dan kunci publik yang digunakan untuk bertukar surat elektronik secara aman sesuai dengan RFC 2350.

9. Asistensi tata kelola keamanan Sistem Elektronik

Badan selaku Kementerian atau Lembaga sektor administrasi pemerintahan telah menyelenggarakan asistensi penyusunan dokumen kebijakan sistem manajemen keamanan informasi, manajemen risiko keamanan, serta audit keamanan kepada Instansi Penyelenggara Negara baik instansi pusat maupun pemerintah daerah. Selain dari sisi kebijakan, diselenggarakan pula asistensi implementasi keamanan pada Sistem Elektronik berdasarkan peraturan perundangan-undangan. Kegiatan tersebut bertujuan untuk meningkatkan profil Keamanan Siber di sektor administrasi pemerintahan dengan memperkuat tata kelola serta implementasinya.

Hasil pembinaan dan pengawasan terhadap sektor administrasi pemerintahan yang telah dilakukan oleh Badan sampai dengan bulan Desember tahun 2024 menghasilkan kesimpulan mengenai kondisi dan profil penerapan pelindungan IIV di sektor administrasi pemerintahan sebagai berikut:

Tabel II.1. Kondisi dan Profil Saat Ini Penerapan Pelindungan IIV di Sektor Administrasi Pemerintahan

Domain	Tingkat Kematangan Keamanan Siber	Keterangan
Identifikasi	level 2	• penerapan Keamanan Siber dalam tahap implementasi yang berulang; • penerapan Keamanan Siber sudah memiliki prosedur yang terorganisir; • penerapan Keamanan Siber bersifat informal; • Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan; dan • dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan.
Proteksi	level 1	• penerapan Keamanan Siber dalam tahap implementasi awal; • penerapan Keamanan Siber belum memiliki prosedur yang terorganisir; • penerapan Keamanan Siber

		bersifat informal; • Keamanan Siber tidak dilakukan secara konsisten dan berkelanjutan; dan • dokumen manajemen risiko dan dokumen kontrol belum disusun.
Deteksi	level 2	• penerapan Keamanan Siber dalam tahap implementasi yang berulang; • penerapan Keamanan Siber sudah memiliki prosedur yang terorganisir; • penerapan Keamanan Siber bersifat informal; • Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan; dan • dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan.
Penanggulangan dan Pemulihan	level 1	• penerapan Keamanan Siber dalam tahap implementasi awal; • penerapan Keamanan Siber belum memiliki prosedur yang terorganisir; • penerapan Keamanan Siber bersifat informal; • Keamanan Siber tidak dilakukan secara konsisten dan berkelanjutan; dan • dokumen manajemen risiko dan dokumen kontrol belum disusun.

E. Analisis Kesenjangan Antara Kondisi Penerapan Kontrol Keamanan Saat Ini dan Kondisi Penerapan yang Ingin Dicapai

Tabel II.2. Analisis Kesenjangan Kondisi Penerapan Kontrol Keamanan IIV di Sektor Administrasi Pemerintahan

Domain	Kategori		Kondisi saat ini Penyelenggara IIV	Kondisi yang diharapkan bagi Penyelenggara IIV	Prioritas peta jalan pelindungan IIV sektor administrasi pemerintahan 2025 - 2029
1	2		3	4	5
Identifikasi	1.1	Mengidentifikasi peran dan tanggung jawab organisasi	level 3	level 4	-
	1.2	Menyusun strategi, kebijakan, dan prosedur pelindungan IIV	level 2	level 4	√
	1.3	Mengelola aset informasi	level 3	level 4	-
	1.4	Menilai dan mengelola risiko Keamanan Siber	level 3	level 4	√
	1.5	Mengelola risiko rantai pasok	level 3	level 4	√
Proteksi	2.1	Mengelola identitas, autentikasi, dan kendali akses	level 3	level 4	-
	2.2	Melindungi aset fisik	level 1	level 3	√
	2.3	Melindungi data	level 3	level 4	-
	2.4	Melindungi aplikasi	level 2	level 3	√
	2.5	Melindungi jaringan	level 3	level 4	-
	2.6	Melindungi sumber daya manusia	level 1	level 3	√
Deteksi	3.1	Mengelola deteksi Peristiwa Siber	level 3	level 4	-
	3.2	Menganalisis anomali dan Peristiwa Siber	level 2	level 3	√
	3.3	Memantau Peristiwa Siber berkelanjutan	level 3	level 4	√

Domain	Kategori		Kondisi saat ini Penyelenggara IIV	Kondisi yang diharapkan bagi Penyelenggara IIV	Prioritas peta jalan pelindungan IIV sektor administrasi pemerintahan 2025 - 2029
Penanggulangan dan Pemulihan	4.1	Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber	level 3	level 4	√
	4.2	Menganalisis dan melaporkan Insiden Siber	level 2	level 3	√
	4.3	Melaksanakan penanggulangan dan pemulihan Insiden Siber	level 3	level 4	–
	4.4	Meningkatkan keamanan setelah terjadinya Insiden Siber	level 1	level 3	√

III. MATRIKS PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR ADMINISTRASI PEMERINTAHAN TAHUN 2025-2029

A. Arah Kebijakan Pelindungan Infrastruktur Informasi Vital

Arah kebijakan pelindungan IIV strategi ditetapkan menjadi 4 (empat) area dengan fokus penerapan pelindungan tertentu, yang meliputi:

1. pemenuhan atau peningkatan kemampuan sektor dalam pengidentifikasian konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV di sektor administrasi pemerintahan. Sasaran penyelenggaraan dalam arah kebijakan ini meliputi kemampuan Penyelenggara IIV untuk:
   a. menyusun strategi, kebijakan, dan prosedur pelindungan IIV;
   b. menilai dan mengelola risiko Keamanan Siber; dan
   c. mengelola risiko rantai pasok.
2. pemenuhan atau peningkatan kemampuan sektor administrasi pemerintahan dalam mencegah, membatasi, dan menahan dampak dari Insiden Siber. Sasaran penyelenggaraan dalam arah kebijakan ini meliputi kemampuan Penyelenggara IIV untuk:
   a. melindungi aset fisik;
   b. melindungi aplikasi; dan
   c. melindungi sumber daya manusia.
3. pemenuhan atau peningkatan kemampuan sektor administrasi pemerintahan dalam memantau secara tepat waktu terjadinya Peristiwa Siber. Sasaran penyelenggaraan dalam arah kebijakan ini meliputi kemampuan Penyelenggara IIV untuk:
   a. menganalisis anomali dan Peristiwa Siber; dan
   b. memantau Peristiwa Siber berkelanjutan.
4. pemenuhan atau peningkatan kemampuan sektor administrasi pemerintahan dalam mengambil tindakan terkait penanggulangan dan pemulihan Insiden Siber. Sasaran penyelenggaraan dalam arah kebijakan ini meliputi kemampuan Penyelenggara IIV untuk:
   a. menyusun perencanaan penanggulangan dan pemulihan Insiden Siber;
   b. menganalisis dan melaporkan Insiden Siber; dan
   c. meningkatkan keamanan setelah terjadinya Insiden Siber.

B. Target Penerapan Kontrol Keamanan

Target penerapan Kontrol Keamanan merupakan nilai capaian yang bertujuan untuk memberikan gambaran kondisi penerapan Keamanan Siber pada Penyelenggara IIV terhadap sasaran penyelenggaraan pelindungan IIV dan domain Kerangka Kerja. Target penerapan Kontrol Keamanan ditentukan berdasarkan hasil pengukuran tingkat kematangan Keamanan Siber yang dibagi menjadi:

1. level 1 (satu), dinamakan level awal;
2. level 2 (dua), dinamakan level berulang;

3. level 3 (tiga), dinamakan level terdefinisi;
4. level 4 (empat), dinamakan level terkelola; dan
5. level 5 (lima), dinamakan level inovatif.

C. Rencana Kerja Penyelenggaraan Pelindungan IIV Sektor Administrasi Pemerintahan Tahun 2025-2029

Rencana kerja pada matriks peta jalan pelindungan IIV sektor administrasi pemerintahan merupakan arah penyelenggaraan IIV berupa kegiatan yang harus dilakukan oleh Penyelenggara IIV. Dalam melaksanakan peta jalan pelindungan IIV sektor administrasi pemerintahan tersebut, Penyelenggara IIV dapat melibatkan pihak lain di luar ekosistem IIV seperti Instansi Penyelenggara Negara yang bukan Penyelenggara IIV, aparat penegak hukum, akademisi, praktisi, masyarakat umum, maupun pihak lain yang terkait. Rencana kerja penyelenggaraan pelindungan IIV sektor administrasi pemerintahan tersebut dituangkan dalam bentuk matriks peta jalan sebagaimana tercantum pada tabel 3.1.

Tabel III.1 Matriks Peta Jalan Pelindungan IIV Sektor Administrasi Pemerintahan Tahun 2025-2029

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan Kontrol Keamanan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
Pemenuhan/ peningkatan kemampuan sektor administrasi pemerintahan dalam mengidentifikasi konteks bisnis, sumber daya, dan risiko yang mendukung Penyelenggaraan IIV	Penyelenggara IIV sektor administrasi pemerintahan mampu menyusun strategi, kebijakan, dan prosedur pelindungan IIV	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah melaksanakan pengukuran tingkat kematangan Keamanan Siber	Melaksanakan pengukuran tingkat kematangan Keamanan Siber secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun	1 program	1 program	1 program	1 program	1 program
		Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 4	Menetapkan dan mengomunikasikan kebijakan Keamanan Siber di lingkungan penyelenggara IIV	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)
			Mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)
			Menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	(level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)
			Menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)
	Penyelenggara IIV pada sektor administrasi pemerintahan mampu menilai dan mengelola risiko Keamanan Siber	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 4	Mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi.	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Menganalisis nilai risiko terhadap IIV	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan Kontrol Keamanan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
			Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Menentukan dan mengomunikasikan toleransi risiko organisasi	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Mengelola hasil penerapan manajemen risiko yang telah ditetapkan	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Melakukan reviu terhadap hasil penerapan manajemen risiko	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 –3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
	Penyelenggara IIV pada sektor administrasi pemerintahan mampu mengelola risiko rantai pasok	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 4	Mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 –3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 –3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan Keamanan Siber pada Penyelenggara IIV	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 –3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 –3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
			Menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 –3,50)	level 4 (3,51 - 3.75)	level 4 (3.76 – 4,00)
Pemenuhan/ Peningkatan kemampuan sektor administrasi	Penyelenggara IIV pada sektor administrasi pemerintahan mampu	Seluruh Penyelenggara IIV sektor administrasi pemerintahan	Menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV	level 2 (1,76 – 2,00)	level 2 (2,01 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan Kontrol Keamanan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
pemerintahan dalam mencegah, membatasi, atau menahan dampak dari ancaman dan/atau insiden siber.	melindungi aset fisik	telah mencapai minimal level 3	Memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)
			Memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)
			Memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)
			Memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 –3,00)	level 3 (3,01 – 3,25)	level 3 (3,26 – 3,50)
	Penyelenggara IIV pada sektor administrasi pemerintahan mampu melindungi aplikasi	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 3	Menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Mengembangkan dan mengimplementasikan rencana manajemen kerentanan	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Mengimplementasikan prosedur pengembangan sistem yang aman	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
	Penyelenggara IIV pada sektor administrasi pemerintahan	Seluruh Penyelenggara IIV sektor administrasi pemerintahan	Menerapkan prosedur pengelolaan keamanan terhadap personel	level 2 (1,76 – 2,00)	level 2 (2,01 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan Kontrol Keamanan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
	mampu melindungi sumber daya manusia	telah mencapai minimal level 3	Menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber	level 2 (1,76 – 2,00)	level 2 (2,01 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)
			Menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia Keamanan Siber yang ada di Penyelenggara IIV	level 2 (1,76 – 2,00)	level 2 (2,01 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)
Pemenuhan/ Peningkatan kemampuan sektor Administrasi Pemerintahan dalam memantau secara tepat waktu terjadinya Peristiwa Siber	Penyelenggara IIV pada sektor administrasi pemerintahan mampu menganalisis anomali dan Peristiwa Siber	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 3	Menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data.	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Menentukan dampak dari Peristiwa Siber yang terdeteksi	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
	Penyelenggara IIV pada sektor administrasi pemerintahan mampu memantau Peristiwa Siber berkelanjutan	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 4	Menerapkan prosedur pendeteksi kode berbahaya dan tak berizin	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)	level 4 (3.76 – 4,00)
			Memonitor kegiatan personel yang berada di dalam lingkup sistem IIV	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)	level 4 (3.76 – 4,00)
			Memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)	level 4 (3.76 – 4,00)
			Menerapkan teknologi pemindaian kerentanan terhadap sistem IIV	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)	level 4 (3.76 – 4,00)

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan Kontrol Keamanan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
Pemenuhan/ Peningkatan kemampuan sektor administrasi pemerintahan dalam tindakan terkait penanggulangan dan pemulihan insiden siber	Penyelenggara IIV pada sektor administrasi pemerintahan mampu menyusun perencanaan penanggulangan dan pemulihan insiden siber	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 4	Menyusun dan menetapkan rencana tanggap insiden siber yang disetujui oleh pimpinan organisasi	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)
			Menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)
			Memastikan rencana tanggap insiden siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)
			Memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap insiden siber dan rencana keberlangsungan kegiatan	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)
			Memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang.	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)	level 4 (3.51 – 3,75)
	Penyelenggara IIV pada sektor administrasi pemerintahan mampu menganalisis dan melaporkan Insiden Siber	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 3	Mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal maupun sumber informasi eksternal	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Memastikan insiden siber dikategorikan sesuai kriteria yang telah ditetapkan	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan Kontrol Keamanan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
	Penyelenggara IIV pada sektor administrasi pemerintahan mampu meningkatkan keamanan setelah terjadinya Insiden Siber	Seluruh Penyelenggara IIV sektor administrasi pemerintahan telah mencapai minimal level 3	Meninjau kembali efektivitas Kontrol Keamanan yang telah diterapkan	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Mengumpulkan dan memelihara hasil forensik digital	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)
			Meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh Tim Tanggap Insiden Siber secara berkala	level 2 (2,00 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,0)	level 3 (3,01 – 3,25)	level 3 (3,26 - 3.50)

IV. PENUTUP

Pelindungan IIV sektor administrasi pemerintahan dilakukan dalam upaya melindungi kepentingan umum dari segala jenis gangguan terhadap IIV sebagai akibat penyalahgunaan informasi elektronik dan transaksi elektronik yang mengganggu ketertiban umum. Gangguan terhadap IIV dapat menimbulkan kerugian dan dampak yang serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, serta perekonomian nasional. Untuk memberikan arah, landasan, dan acuan bagi Penyelenggara IIV sektor administrasi pemerintahan, maka perlu disusun peta jalan pelindungan IIV sektor administrasi pemerintahan tahun 2025-2029. Terlaksananya peta jalan pelindungan IIV sektor administrasi pemerintahan ini dapat diwujudkan melalui sinergi dan kolaborasi antara Badan selaku Kementerian atau Lembaga dan Instansi Penyelenggara Negara sebagai Penyelenggara IIV sektor administrasi pemerintahan.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN