PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA
NOMOR 34 TAHUN 2025
TENTANG
PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL
SEKTOR PERTAHANAN TAHUN 2025 – 2029

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PERTAHANAN REPUBLIK INDONESIA,

Menimbang : a. bahwa sistem elektronik yang mendukung infrastruktur informasi vital sektor pertahanan memiliki peran strategis dalam menjaga keamanan nasional, sehingga perlu dilakukan pelindungan secara terencana dan berkesinambungan;

b. bahwa untuk menjamin keberlangsungan operasional dan mencegah gangguan, kerusakan, atau kehancuran akibat ancaman siber terhadap infrastruktur informasi vital sektor pertahanan, diperlukan penyusunan peta jalan pelindungan infrastruktur informasi vital sektor pertahanan yang komprehensif;

c. bahwa berdasarkan ketentuan Pasal 8 ayat (1) Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, Kementerian Pertahanan menyusun dan menetapkan peta jalan pelindungan infrastruktur informasi vital sektor pertahanan untuk jangka waktu 5 (lima) tahun;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Menteri Pertahanan tentang Peta Jalan Pelindungan Infrastruktur Informasi Vital Sektor Pertahanan Tahun 2025 – 2029;

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 106, Tambahan Lembaran Negara Republik Indonesia Nomor 4916) sebagaimana telah diubah dengan Undang-Undang Nomor 61 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 225, Tambahan Lembaran Negara Republik Indonesia Nomor 6994);

3. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 128);
4. Peraturan Presiden Nomor 151 Tahun 2024 tentang Kementerian Pertahanan (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 347) sebagaimana telah diubah dengan Peraturan Presiden Nomor 85 Tahun 2025 tentang Perubahan atas Peraturan Presiden Nomor 151 Tahun 2024 tentang Kementerian Pertahanan (Lembaran Negara Republik Indonesia Tahun 2025 Nomor 121);
5. 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);
6. Peraturan Menteri Pertahanan Nomor 1 Tahun 2024 tentang Organisasi dan Tata Kerja (Berita Negara Republik Indonesia Tahun 2024 Nomor 75);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PERTAHANAN TENTANG PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR PERTAHANAN TAHUN 2025-2029.

Pasal 1

Dalam Peraturan Menteri 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 senciiri 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. Peta Jalan Pelindungan Infrastruktur Informasi Vital Sektor Pertahanan Tahun 2025-2029 yang selanjutnya disebut Peta Jalan Pelindungan IIV Sektor Pertahanan adalah dokumen rencana kerja IIV sebagai pedoman dalam perencanaan persiapan serta pelaksanaan penyelenggara IIV Sektor Pertahanan dalam menyelenggarakan pelindungan IIV di masing-masing unit organisasi di sektor pertahanan serta industri pertahanan.
3. Penyelenggara IIV Sektor Pertahanan yang selanjutnya disebut Penyelenggara IIV adalah unit organisasi, satuan kerja, dan/atau badan usaha yang memiliki dan/atau mengoperasikan IIV dalam lingkup sektor Pertahanan.
4. 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 yang bersifat teknis maupun sosial.

5. Sektor Pertahanan adalah suatu lingkungan, usaha dan sumber daya di bidang pertahanan untuk mendukung pertahanan negara.
6. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
7. Kementerian Pertahanan yang selanjutnya disebut Kemhan adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pertahanan.

Pasal 2

(1) Ruang lingkup Peta Jalan Pelindungan IIV Sektor Pertahanan memuat:
   a. analisis lingkungan strategis penyelenggaraan pelindungan IIV Sektor Pertahanan;
   b. arah kebijakan pelindungan IIV;
   c. sasaran penyelenggaraan pelindungan IIV Sektor Pertahanan;
   d. target penerapan Kontrol Keamanan pelindungan IIV Sektor Pertahanan; dan
   e. rencana kerja penyelenggaraan pelindungan IIV Sektor Pertahanan.
(2) Peta Jalan Pelindungan IIV Sektor Pertahanan sebagaimana dimaksud pada ayat (1) berlaku untuk periode tahun 2025 sampai dengan tahun 2029.
(3) Peta Jalan Pelindungan IIV Sektor Pertahanan sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 3

(1) Kemhan melakukan reviu terhadap Peta Jalan Pelindungan IIV Sektor Pertahanan setiap tahun.
(2) Dalam hal berdasarkan hasil reviu sebagaimana dimaksud pada ayat (1) diperlukan perubahan, Menteri menetapkan perubahan Peta Jalan Pelindungan IIV Sektor Pertahanan.

Pasal 4

(1) Penyelenggara IIV harus melaksanakan Peta Jalan Pelindungan IIV Sektor Pertahanan sebagaimana dimaksud dalam Pasal 2.
(2) Dalam melaksanakan Peta Jalan Pelindungan IIV Sektor Pertahanan sebagaimana dimaksud pada ayat (1), Penyelenggara IIV berkoordinasi dengan Kemhan melalui satuan kerja yang menangani bidang Keamanan Siber.
(3) Pelaksanaan Peta Jalan Pelindungan IIV Sektor Pertahanan sebagaimana dimaksud pada ayat (1) disesuaikan dengan kapasitas setiap Penyelenggara IIV dan kondisi situasional sektor pertahanan.

Pasal 5

(1) Kemhan melakukan pembinaan dan pengawasan terhadap pelaksanaan Peta Jalan Pelindungan IIV Sektor Pertahanan sebagaimana dimaksud dalam Pasal 2.

(2) Pembinaan sebagaimana dimaksud pada ayat (1) meliputi kegiatan:
   a. koordinasi peningkatan kapasitas sumber daya manusia yang ada di Sektor Pertahanan;
   b. penyelenggaraan simulasi tanggap Insiden Siber untuk lingkup sektor yang diikuti oleh seluruh Penyelenggara IIV Sektor Pertahanan;
   c. forum analisis dan berbagi informasi Keamanan Siber dalam lingkup Sektor Pertahanan;
   d. koordinasi teknis penyelenggaraan pelindungan IIV dalam lingkup Sektor Pertahanan; dan/atau
   e. kegiatan lain yang dibutuhkan Penyelenggara IIV Sektor Pertahanan.

(3) Pengawasan sebagaimana dimaksud pada ayat (1) meliputi kegiatan:
   a. Penerimaan dan verifikasi laporan penerapan Peta Jalan Pelindungan IIV Sektor Pertahanan yang dilakukan oleh Penyelenggara IIV; dan
   b. evaluasi implementasi Peta Jalan Pelindungan IIV Sektor Pertahanan berdasarkan hasil pengukuran tingkat kematangan Keamanan Siber.

(4) Berdasarkan hasil pembinaan dan pengawasan sebagaimana dimaksud pada ayat (2) dan ayat (3), Kemhan menyusun rencana kerja.

(5) Rencana kerja sebagaimana dimaksud pada ayat (4) disusun oleh satuan kerja yang menangani bidang Keamanan Siber.

(6) Satuan kerja sebagaimana dimaksud pada ayat (5) dapat melibatkan pihak lain yang diperlukan dalam penyusunan rencana kerja.

(7) Rencana kerja sebagaimana dimaksud pada ayat (4) ditetapkan oleh Menteri.

Pasal 6

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Jakarta
pada tanggal 22 Desember 2025

MENTERI PERTAHANAN
REPUBLIK INDONESIA,

Cap/tertanda

SJAFRIE SJAMSOEDDIN

Diundangkan di Jakarta
pada tanggal 31 Desember 2025

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM REPUBLIK INDONESIA,

Cap/tertanda

DHAHANA PUTRA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2025 NOMOR 1264

Autentikasi
Kepala Biro Tata Usaha dan Protokol
Setjen Kemhan

Charles Alling S.E., M.MDS.
Brigadir Jenderal TNI

LAMPIRAN
PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA
NOMOR ... TAHUN ...
TENTANG PETA JALAN PELINDUNGAN INFRASTRUKTUR
INFORMASI VITAL SEKTOR PERTAHANAN TAHUN 2025-2029

PETA JALAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL SEKTOR PERTAHANAN TAHUN 2025-2029

BAB I
GAMBARAN UMUM

1.1 Pendahuluan

Perkembangan pesat teknologi, informasi, dan komunikasi telah menyebabkan perubahan pola hidup manusia. Dalam hal penggunaan teknologi, informasi, dan komunikasi melalui pemanfaatan jaringan internet, dari perspektif ancaman siber dan anatomi gangguan secara nasional, hal ini akan berbanding lurus dengan peningkatan dinamika aktivitas ancaman dan serangan siber.

Teknologi Internet saat ini telah dimanfaatkan oleh berbagai pihak baik personal, masyarakat, akademisi, industri, dan institusi, termasuk sektor pertahanan, dalam mencari, mendapatkan, mengelola, menerima, dan mengirimkan informasi. Aspek-aspek dalam kehidupan berbangsa dan bernegara seperti ideologi, politik, ekonomi, sosial, budaya, pertahanan, dan keamanan terpengaruh sangat tinggi dengan akselerasi internet saat ini sehingga meningkatkan potensi ancaman dan serangan siber, termasuk terhadap keberlangsungan penyelenggaraan IIV. Sumber ancaman dan serangan siber tersebut dapat berasal dari kegiatan intelijen, penyelidikan, organisasi ekstrem, peretasan, kriminalitas, frustrasi, persaingan, konflik, serta perkembangan teknologi itu sendiri. Bentuk ancaman siber yang dimaksud antara lain upaya membobol kerahasiaan informasi, merusak sistem elektronik, penyalahgunaan komputer, kejahatan perbankan, terorisme, dan tindakan lainnya yang makin sulit untuk ditanggulangi.

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

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

Dalam Peraturan Presiden tersebut, sektor pertahanan merupakan salah satu sektor yang ditetapkan sebagai sektor IIV dan Kemhan ditetapkan sebagai kementerian yang bertugas mengawasi dan mengeluarkan pengaturan terhadap Sektor Pertahanan. Untuk itu, Kemhan menyusun dan menetapkan Peta Jalan Pelindungan IIV Sektor

Pertahanan guna memberi arah dan langkah perencanaan serta pelaksanaan bagi Penyelenggara IIV dalam menyelenggarakan pelindungan IIV Sektor Pertahanan.

1.2 Tujuan

Peta Jalan Pelindungan IIV Sektor Pertahanan bertujuan menjadi acuan yang memberi arah untuk langkah perencanaan dan pelaksanaan bagi:

a. Kemhan untuk mengawasi dan mengeluarkan pengaturan terhadap Sektor Pertahanan; dan
b. Penyelenggara IIV dalam menyelenggarakan pelindungan IIV Sektor Pertahanan Tahun 2025-2029.

1.3 Ruang Lingkup

Ruang lingkup Peta Jalan Pelindungan IIV Sektor Pertahanan terdiri atas:

a. gambaran umum;
b. analisis lingkungan strategis penyelenggaraan pelindungan IIV Sektor Pertahanan;
c. arah kebijakan;
d. sasaran penyelenggaraan;
e. target penerapan Kontrol Keamanan;
f. rencana kerja penyelenggaraan pelindungan IIV Sektor Pertahanan; dan
g. penutup.

BAB II
ANALISIS LINGKUNGAN STRATEGIS PENYELENGGARAAN PELINDUNGAN IIV SEKTOR PERTAHANAN

Analisis lingkungan strategis penyelenggaraan pelindungan IIV di maksudkan untuk menggambarkan kondisi penerapan kontrol keamanan saat ini di Sektor Pertahanan meliputi: Karakteristik layanan vital, Analisis dampak gangguan dan kegagalan penyelenggaraan IIV, Identifikasi Regulasi pelindungan IIV, Analisis kondisi saat ini dalam penerapan pelindungan IIV Sektor Pertahanan dan Analisis kesenjangan kondisi penerapan kontrol keamanan IIV Sektor Pertahanan.

2.1 Karakteristik layanan vital sektor pertahanan.

Pelindungan IIV pada sektor pertahanan dilakukan terhadap sistem elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan sistem elektronik lainnya dalam menunjang sektor pertahanan yang terdiri atas sistem komputer, aplikasi maupun jaringan, baik berbentuk fisik maupun virtual yang sangat vital, dimana gangguan terhadapnya berpotensi mengancam kerahasiaan/keamanan, keutuhan dan ketersediaan data serta informasi bagi kepentingan taktis dan strategis di sektor pertahanan. Adapun karakteristik layanan vital di Sektor Pertahanan yakni layanan yang:

a. berdampak langsung mempengaruhi kemampuan negara dalam menjaga dan melindungi kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap Bangsa;

b. memuat data atau informasi yang berkaitan dengan sistem pertahanan negara;

c. tidak dapat tergantikan tanpa mengganggu kemampuan militer dalam menjalankan operasi strategis maupun taktis;

d. diselenggarakan untuk mengelola dan menyimpan data atau informasi rahasia negara terkait sistem pertahanan negara;

e. jika terganggu dapat menyebabkan gangguan yang meluas terhadap sektor lain;

f. terkait dengan rantai pasokan atau infrastruktur industri pertahanan yang berpengaruh langsung pada kemampuan sistem pertahanan negara.

2.2 Analisis dampak gangguan dan kegagalan penyelenggaraan IIV Sektor Pertahanan.

Kemajuan TIK juga memberikan tantangan tersendiri di sektor pertahanan seperti tantangan terhadap proses modernisasi teknologi dan pengelolaan infrastruktur digital. Dengan kondisi tersebut juga memiliki dampak risiko yang dapat muncul dan menargetkan sistem pertahanan di Indonesia.

Fakta menunjukan bahwa ancaman keamanan siber di sektor pertahanan cukup tinggi, sesuai hasil Monitoring Data Pushansiber Bainstrahan Kemhan tentang catatan ancaman pada tahun 2023 dan 2024 sebagai berikut:

a. Januari s.d Desember 2023: 12.406.662 kasus.
b. Januari s.d Desember 2024: 9.463.546 kasus

Pelindungan IIV sektor pertahanan merupakan unsur utama bagi keberlanjutan fungsi strategis pertahanan negara. Gangguan atau kegagalan pada pelindungan IIV sektor pertahanan ini dapat memberikan dampak yang sangat signifikan, baik pada tingkat operasional militer, stabilitas pertahanan Negara, hingga reputasi internasional Indonesia. Dalam konteks keamanan siber Indonesia, yang terus menghadapi tantangan di tengah dinamika ancaman global, kerentanan terhadap IIV sektor pertahanan harus menjadi perhatian utama.

Potensi dampak yang dipertimbangkan dalam pelaksanaan pelindungan IIV berfokus kepada dampak level nasional, namun dengan tidak mengesampingkan pula pertimbangan pada seluruh level dampak yang memiliki potensi eskalasi pada level nasional. Gangguan, kegagalan, kerusakan, dan/atau kehancuran pada suatu sektor atau layanan IIV, dapat diakibatkan oleh salah satu atau kombinasi dari kategori dampak berikut:

a. dampak operasional adalah berbagai akibat yang ditimbulkan karena kegagalan, tidak memadainya prosedur, kesalahan orang, sistem, atau sumber eksternal yang mempengaruhi kondisi atau keberlangsungan layanan baik dalam ruang lingkup instansi atau institusi, sektoral, dan berpotensi berdampak pada level nasional;

b. 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 mempengaruhi kondisi, keberlangsungan layanan baik dalam lingkup instansi atau institusi, sektoral, dan berpotensi berdampak pada level nasional;

c. 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 pertahanan dan keamanan nasional.

d. 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 dapat dipahami sebagai keterhubungan di antara infrastruktur dalam kondisi suatu layanan berkaitan dalam hal keadaan ataupun menunjang layanan lainnya.

Dampak terjadinya gangguan atau kegagalan penyelenggaraan pelindungan IIV sektor pertahanan juga mempertimbangkan dampak pada integritas, aksesibilitas, dan verifikasi data dalam sistem pertahanan yang dapat menimbulkan sejumlah konsekuensi serius sebagai berikut:

a. Dampak langsung terhadap keamanan nasional yang mana hal ini akan berimplikasi terhadap operasional sektor pertahanan seperti:

1) ketidakakuratan data mengakibatkan keputusan strategis yang tidak tepat.

2) komunikasi yang terputus atau terganggu antar unit dapat menghambat operasi pertahanan negara.

3) kerusakan peralatan militer atau infrastruktur dapat mengakibatkan terganggunya sistem alutsista sehingga menimbulkan kerugian finansial yang besar.

b. Kerentanan serangan siber

1) pencurian data sensitif, data rahasia militer, rencana operasi, dan informasi inteljen dapat dengan mudah dicuri oleh pihak yang tidak berwenang.

2) sabotase sistem, sistem kendali senjata, komunikasi, dan infrastruktur kritis dikompromikan, dapat mengakibatkan disfungsi atau kerusakan terhadap penyelenggaraan IIV Sektor Pertahanan.

3) disinformasi, informasi palsu atau menyesatkan dapat disebarluaskan untuk membingungkan negara/pemerintah.

c. Hilangnya kepercayaan

1) kegagalan dalam melindungi data sensitif dapat menurunkan tingkat kepercayaan publik terhadap kemampuan militer dalam menjaga pertahanan negara.

2) kepercayaan forum internasional dapat menurun, sehingga menghambat kerja sama militer multilateral.

2.3 Identifikasi Regulasi pelindungan IIV Sektor Pertahanan

Dalam penyelenggaraan pelindungan IIV sektor pertahanan, terdapat beberapa peraturan perundang-undangan yang mengatur, terkait dengan hal tersebut, antara lain:

a. Undang-undang Nomor 3 tahun 2002 tentang pertahanan negara

Undang-undang Nomor 3 tahun 2002 tentang pertahanan negara telah menentukan penerapan sistem pertahanan semesta yang melibatkan seluruh komponen bangsa, baik pemerintah, TNI, masyarakat, maupun sektor lain, untuk terlibat secara aktif dalam menjaga kedaulatan dan keutuhan wilayah negara dalam menghadapi ancaman yang bersifat militer maupun non militer.

Salah satu bentuk ancaman non militer adalah serangan siber terhadap sistem pertahanan negara sehingga diperlukan pelindungan IIV sektor pertahanan, yang mencakup berbagai sistem informasi dan infrastruktur strategis, sebagai bagian integral dari upaya menjaga kedaulatan negara dan stabilitas pertahanan nasional.

Pelindungan IIV sektor pertahanan, meliputi sistem komunikasi, data intelijen, serta alutsista yang terhubung dengan jaringan digital, harus dilindungi dari berbagai ancaman yang dapat mengganggu operasional pertahanan, termasuk ancaman yang dapat mengganggu operasional pertahanan, termasuk ancaman siber yang semakin berkembang.

b. Undang-undang Nomor 3 tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia.

Undang-undang Nomor 3 tahun 2025 tentang tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia secara tegas mengamanatkan salah satu tugas pokok TNI dalam OMSP (Operasi Militer Selain Perang) adalah membantu dalam upaya menanggulangi ancaman pertahanan siber. Dalam Penjelasan atas Undang-Undang Republik Indonesia Nomor 3 Tahun 2025 tentang Perubahan atas Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, yang dimaksud dengan membantu dalam upaya menanggulangi ancaman Pertahanan Siber, TNI berperan serta dalam Upaya menanggulangi ancaman pertahanan siber pada sektor pertahanan (*cyber defense*).

Dalam menjalankan tugas ini, TNI akan fokus melindungi sistem pertahanan nasional dari ancaman siber yang dapat membahayakan keamanan negara, diantaranya melaksanakan operasi siber. Untuk memastikan bahwa operasi siber yang dilakukan tidak melanggar hak masyarakat dalam mengakses informasi, TNI akan senantiasa melakukan koordinasi dengan instansi terkait.

c. Undang- Undang Nomor 1 tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik.

Perubahan yang ada pada pasal eksisting di UU ITE Nomor 1 tahun 2024 merupakan penyempurnaan norma pada UU Nomor 19 tahun 2016 tentang perubahan atas UU Nomor 11 tahun 2008. Penyempurnaan tersebut dilakukan untuk memberikan kepastian hukum dan perlindungan bagi masyarakat dalam ruang digital. Peraturan ini mengatur tentang:

1) Penyempurnaan pasal kontroversial: Beberapa pasal yang sebelumnya dianggap multitafsir, seperti pasal terkait penghinaan atau pencemaran nama baik, telah di ubah pasal 27 sekarang membahas penyerangan kehormatan atau nama baik melalui media elektronik dengan ketentuan yang lebih jelas, sementara pasal 29 menyederhanakan ancaman kekerasan yang dikirim secara elektronik.
2) Perlindungan anak: UU ini memperkenalkan ketentuan baru terkait perlindungan anak dalam ruang digital. Penyelenggara sistem Elektronik (PSE) diwajibkan untuk memastikan perlindungan anak dengan langkah-langkah seperti verifikasi usia dan mekanisme pelaporan penyalahgunaan.
3) Identitas digital dan sertifikasi elektronik: pasal baru ditambahkan untuk mengatur identitas digital, yang bertujuan meningkatkan keamanan dan keandalan transaksi elektronik.
4) Peningkatan peran pemerintah: Dalam UU yang baru, peran pemerintah semakin diperkuat, dengan pembentukan dewan kebijakan Nasional perlindungan data pribadi serta pengawasan ekosistem digital yang aman dan inovatif.

d. Undang-Undang Nomor 16 tahun 2012 tentang Industri Pertahanan.

Undang-Undang Nomor 16 tahun 2012 tentang industri pertahanan mengatur berbagai aspek yang mendukung pembangunan industri pertahanan nasional. UU ini menetapkan bahwa industri pertahanan terdiri dari Badan Usaha milik negara (BUMN), Badan usaha milik swasta (BUMS), serta lembaga riset dan pengembangan yang terintegritas dalam penyediaan alat utama sistem senjata (alutsista) dan perlengkapan pertahanan. Salah satu tujuan undang-undang ini untuk menciptakan kemandirian pertahanan industri dalam negeri pada pemenuhan alat peralatan pertahanan dan keamanan dengan menekankan pentingnya penguasaan teknologi dan innovasi yang mencakup aspek teknologi informasi dan siber.

Kemandirian pertahanan dan keamanan memerlukan tekad dan keterpaduan upaya dari semua pihak, serta didukung oleh kebijakan Pemerintah dalam pemberdayaan segenap potensi sumber daya nasional, termasuk perangkat regulasi. Salah satu perwujudan kemandirian pertahanan adalah kemandirian di bidang pemenuhan kebutuhan Alat Peralatan Pertahanan dan Keamanan. Dalam membangun kemandirian tidak terlepas dari peran Industri Pertahanan sebagai pelaku dalam pemanfaatan, penguasaan dan pengembangan teknologi pertahanan dan keamanan yang terpilih.

e. Peraturan pemerintah Nomor 141 tahun 2015 tentang Pengelolaan Idustri Pertahanan.

Dalam peraturan pemerintah ini telah diatur tata kelola mulai dari peningkatan sumber daya manusia, rancang bangun dan perekayasaan, pengembangan desain dan produk sampai dengan pemeliharaan, perbaikan dan modifikasi.

Salah satu tanggung jawab industri pertahanan adalah untuk membangun kemampuan dalam menghasilkan alpalhankam yang andal dan tangguh untuk melindungi seluruh wilayah negara kesatuan republik Indonesia. Kemampuan sumber daya manusia dan teknologi pada industri pertahanan merupakan potensi bangsa yang harus disinergikan dalam rangka mencapai tujuan yaitu kemandirian industri pertahanan.

f. Peraturan presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital.

Peraturan presiden (perpres) Nomor 82 tahun 2022 merupakan landasan hukum untuk pelindungan infrastruktur informasi vital di indonesia yang mencakup berbagai sektor strategis, termasuk pertahanan, keamanan, energi, transportasi, dan sektor lain yang memiliki dampak signifikan terhadap keselamatan masyarakat, keamanan nasional, serta perekonomian. Perpres ini mengatur kerangka identifikasi, penetapan, dan pengelolaan IIV, dengan tujuan memastikan keberlangsungan layanan penting, mitigasi risiko gangguan, serta pemulihan pasca-insiden.

Salah satu poin penting dalam perpres ini adalah peran pemerintah dalam menetapkan daftar IIV dan tanggung jawab penyelenggara sistem elektronik untuk mematuhi standar keamanan yang di tetapkan. Perpres juga menekankan kolaborasi antara kementrian/lembaga, sektor swasta, dan instansi terkait

dalam menyusun langkah strategis pelindungan IIV, termasuk pengembangan sistem deteksi dini, penguatan kapasitas tanggap darurat, dan pembentukan kerangka audit berkala. Dengan implementasi yang efektif, perpres ini diharapkan dapat meningkatkan resiliensi nasional terhadap ancaman siber yang semakin kompleks dan menjaga keberlanjutan layanan penting yang menjadi tulang punggung stabilitas negara.

g. Peraturan presiden Nomor 47 tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.

Peraturan ini dimaksudkan untuk mengatur strategi keamanan siber nasional serta manajemen krisis siber, mengingat pentingnya keamanan siber dalam menjaga stabilitas dan keamanan negara. Peraturan ini bertujuan untuk mengembangkan dan memantapkan strategi keamanan siber nasional guna melindungi infrastruktur kritikal, data sensitif, dan sumber daya nasional dari ancaman siber. Selain itu, peraturan ini juga bertujuaan untuk meningkatkan kemampuan negara dalam menghadapi krisis siber, meningkatkan ketahanan keamanan siber nasional dan menghadapi ancaman siber yang semakin kompleks. 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. Fokus area strategi Keamanan Siber Nasional salah satunya adalah Penguatan pelindungan infrastruktur informasi vital yang meliputi:

1) penyelenggaraan pelindungan infrastruktur informasi vital; dan

2) peningkatan pembinaan dan pengawasan penyelenggaraan pelindungan informasi vital.

g. Peraturan menteri pertahanan nomor 2 tahun 2024 tentang Kebijakan Pertahanan Negara tahun 2024.

Peraturan menteri pertahanan nomor 2 tahun 2024 tentang kebijakan pertahanan negara tahun 2024 menetapkan panduan strategis untuk menghadapi dinamika ancaman global, regional, dan nasional. Dokumen ini menyoroti pentingnya modernisasi alat utama sistem senjata (alutsista), penguatan kemampuan siber dan inteljen, serta optimalisasi kerja sama internasional guna memperkuat posisi indonesia dalam menjaga kedaulatan dan keamanan nasional. Pendekatan ini dilandasi oleh ancaman hibrida, yang mencakup serangan fisik hingga siber, yang menuntut kesiapsiagaan lintas sektor.

Kebijakan ini juga mencakup aspek ketahanan sumber daya nasional, meliputi pertahanan wilayah, pemanfaatan teknologi tinggi dalam sektor pertahanan, serta memperdayaan masyarakat untuk mendukung konsep pertahanan semesta. Pendekatan pertahanan semesta juga diintegrasikan, dengan penekanan pada pemberdayaan masyarakat serta pengelolaan sumber daya nasional secara efektif untuk mendukung pertahanan negara. Fokus khusus diberikan pada pelindungan infrastruktur informasi vital, yang menjadi bagian penting dalam menjaga stabilitas sistem nasional di tengah ancaman digital. Kebijakan ini di rancang untuk

mewujudkan pertahanan yang adaptif, inovatif, dan terintegrasi, selaras dengan kebutuhan zaman dan tantangan modern.

2.4 Identifikasi Kegiatan Pelindungan yang telah ditetapkan pada Layanan Vital dari aspek Ketersediaan dan Kamampuan Sumber Daya Manusia, Tata Kelola dan Teknologi.

Penyelenggaraan IIV pada sektor pertahanan telah diterapkan dengan memberdayakan sarana serta situasi dan kondisi yang dimiliki.

a. Sumber daya manusia.

Pelindungan IIV di lingkungan Kemhan melibatkan para ahli siber dan operator layanan vital di Pushansiber, Pusdatin, Bagdatin Satker Kemhan yang terampil dan menguasai ilmu pengetahuan dan teknologi di bidang Keamanan Siber serta berintegritas.

Pelindungan IIV di lingkungan TNI melibatkan para ahli siber dan operator layanan vital di Satsiber TNI, Pussansiad, Labpamsisjar Dispamsanal, Satsiber Dispamsanau, dan Satker-satker TNI yang terampil dan menguasai ilmu pengetahuan dan teknologi di bidang Keamanan Siber serta berintegritas.

Pelindungan IIV di lingkungan Inhan melibatkan para ahli siber dan operator layanan vital di masing-masing Inhan yang terampil dan menguasai ilmu pengetahuan dan teknologi di bidang Keamanan Siber serta berintegritas.

b. Tata kelola.

1) Kebijakan Keamanan Siber.

a) Kebijakan penyelenggaraan keamanan siber di sektor pertahanan saat ini masih berpedoman pada peraturan menteri pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber, regulasi terbaru sebagaimana diamanatkan oleh peraturan presiden Nomor 82 Tahun 2022 tentang pelindungan IIV masih dalam proses penyusunan.

b) Dalam penyelenggaraan Keamanan Siber, Kemhan dan TNI serta Inhan, senantiasa melakukan evaluasi dan pembenahan melalui penguatan ekosistem Keamanan Siber yang mencakup sumber daya manusia, proses, dan teknologi serta peningkatan sinergi dan kolaborasi.

c) Penyelenggara IIV sektor Pertahanan terdiri dari, namun tidak terbatas pada:

(1) UO Mabes TNI.
(2) UO TNI AD.
(3) UO TNI AL.
(4) UO TNI AU.
(5) Industri Pertahanan.
(6) Unit kerja/satuan kerja yang memiliki tugas dan fungsi untuk mendukung Pertahanan Negara.

d) Manajemen Risiko

(1) Penilaian Risiko: UO Kemhan, UO TNI dan Inhan telah melakukan penilaian risiko secara terbatas terhadap ancaman dan kerentanan menggunakan sarana yang tersedia.

(2) Pengelolaan Risiko: UO Kemhan, UO TNI dan Inhan melakukan pengembangan strategi untuk mengelola risiko, termasuk pencegahan, mitigasi, transfer, dan penerimaan risiko sesuai dengan situasi dan kondisi.

e) Kepatuhan dan Regulasi

(1) Kepatuhan terhadap Regulasi. UO Kemhan, UO TNI dan Inhan telah mematuhi regulasi dan standar keamanan yang berlaku antara lain; ISO 27001, GDPR, atau NIST.

(2) Audit dan Penilaian. UO Kemhan, UO TNI dan Inhan secara terbatas telah melakukan audit dan penilaian untuk memastikan kepatuhan terhadap kebijakan dan regulasi.

f) Kesadaran dan Pelatihan

(1) Pelatihan Keamanan: UO Kemhan, UO TNI dan Inhan secara terbatas telah memberikan sosialisasi maupun pelatihan keamanan kepada para pegawai/karyawan untuk meningkatkan kesadaran akan ancaman siber dan praktik keamanan terbaik.

(2) Program Kesadaran: UO Kemhan, UO TNI dan Inhan secara terbatas telah mengadakan program kesadaran keamanan untuk mengedukasi pegawai/karyawan tentang pentingnya keamanan informasi.

g) Tanggap Insiden

(1) Rencana Tanggap Insiden: UO Kemhan, UO TNI dan Inhan secara terbatas telah mengembangkan dan mendokumentasikan rencana tanggap insiden untuk merespons dan mengatasi insiden keamanan.

(2) Tim Tanggap Insiden: UO Kemhan, UO TNI dan Inhan telah membentuk tim tanggap insiden yang terlatih untuk menangani insiden keamanan dengan cepat dan efisien.

h) Pemantauan dan Pengujian

(1) Pemantauan Sistem: UO Kemhan, UO TNI dan Inhan secara terbatas telah melakukan pemantauan berkelanjutan terhadap sistem dan jaringan untuk mendeteksi aktivitas yang mencurigakan atau tidak sah.

(2) Pengujian Keamanan: UO Kemhan, UO TNI dan Inhan secara terbatas telah melakukan pengujian keamanan secara berkala, seperti uji penetrasi atau audit keamanan, untuk mengidentifikasi kelemahan dan kerentanan.

i) Manajemen Identitas dan Akses

(1) Kontrol Akses: UO Kemhan, UO TNI dan Inhan secara terbatas telah menerapkan kontrol akses untuk membatasi akses ke sistem dan data hanya kepada individu yang berwenang.

(2) Manajemen Identitas: UO Kemhan, UO TNI dan Inhan secara terbatas telah mengelola identitas digital dan hak akses pengguna dengan efektif untuk memastikan bahwa hanya individu yang sah yang dapat mengakses informasi sensitif.

c. Teknologi.

Untuk melindungi IIV dari ancaman atau serangan siber, setiap unit organisasi telah memiliki fasilitas teknologi berupa perangkat keras dan perangkat lunak yang memiliki fungsi meliputi identifikasi, proteksi, deteksi, penanggulangan dan pemulihan. Sistem dan peralatan yang saat ini digunakan di sektor pertahanan antara lain:

1) Identifikasi

- *Vulnerability assesment & penetration test* adalah pendekatan yang digunakan dalam keamanan siber untuk mengidentifikasi dan mengatasi kerentanan serta potensi risiko keamanan dalam sistem jaringan, atau aplikasi.

2) Proteksi

a) *Network security* merupakan konsep dan praktik yang bertujuan untuk melindungi integritas, kerahasiaan, dan ketersediaan data serta sumber daya dalam jaringan komputer.

b) *End point protection* merupakan *tools* keamanan siber untuk melindungi perangkat akhir (*end point*) seperti komputer, laptop, ponsel, dan tablet dari serangan siber dan ancaman *malware.*

c) *Instrusion detection and prevention system* (IDPS) adalah sistem keamanan siber yang dirancang untuk mendeteksi dan mencegah ancaman terhadap jaringan atau sistem komputer. *Instrusion detection system* (IDS) dan *intrusion prevention system* (IPS), sehingga tidak hanya mengidentifikasi potensi serangan tetapi juga mengambil tindakan untuk menghentikannya secara otomatis.

3) Deteksi

a) *Cyber threat intelligence.* Merupakan alat yang di gunakan untuk proses pengumpulan, analisis, dan distribusi informasi yang berkaitan dengan ancaman dan risiko keamanan siber.

b) *Security information and event managemen* (SIEM) adalah perangkat lunak atau platform yang dirancang untuk membantu mengelola dan mengamati keamanan sistem komputer dan jaringan.

4) Penanggulangan dan Pemulihan.

a) Penanggulangan:

(1) Pembentukan tim tanggap insiden siber.

(2) *Digital forensic* adalah perangkat lunak atau *platform* yang digunakan oleh profesional keamanan siber dan investigasi forensik digital untuk mengumpulkan, menganalisis, dan merespons insiden keamanan siber.

(3) *Security Orchestration Automation and Response* (SOAR) adalah platform keamanan yang mengintegrasikan data dari berbagai alat keamanan untuk mengotomatiskan dan mempercepat respon terhadap ancaman.

b) Pemullihan

- Penyiapan sistem cadangan sebagai backup dari sistem utama untuk meningkatkan keberlangsungan sistem dan pemulihan dari serangan siber.

2.5 Analisis kesenjangan kondisi penerapan kontrol keamanan saat ini dan kondisi penerapan kontrol keamanan yang ingin dicapai.

Dalam rangka pembuatan Peta Jalan Pelindungan IIV Sektor Pertahanan Tahun 2025-2029 perlu diperhatikan beberapa hal yang menjadi kesenjangan dari kondisi awal dihadapkan dengan kondisi yang diharapkan ditinjau dari aspek; identifikasi, proteksi, deteksi dan penanggulangan serta pemulihan yang tertuang dalam tabel II.1:

Tabel II.1. Analis Kesenjanagan Kondisi Penerapan Kontrol Keamanan IIV Sektor Pertahanan

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

1	2		3	4	5
Penanggulangan dan Pemulihan	4.1	Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber	level 1	level 3	√
	4.2	Menganalisis dan melaporkan Insiden Siber	level 2	level 3	√
	4.3	Melaksanakan penanggulangan dan pemulihan Insiden Siber	level 2	level 3	–
	4.4	Meningkatkan keamanan setelah terjadinya Insiden Siber	level 2	level 3	√

BAB III
ARAH KEBIJAKAN DAN TARGET PENERAPAN KONTROL KEAMANAN PELINDUNGAN IIV SEKTOR PERTAHANAN

3.1 Arah kebijakan pelindungan infrastruktur informasi vital.

Untuk mewujudkan pencapaian Keamanan dan Ketahanan Siber bagi kepentingan Sistem Pertahanan Negara, maka arah kebijakan penyelenggaraan Pelindungan IIV Sektor Pertahanan pada tahun 2025 – 2029 ditentukan sebagai berikut:

a. Peningkatan kemampuan sektor dalam mengidentifikasi konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV di sektor pertahanan.

b. Peningkatan kemampuan sektor dalam mencegah, membatasi, dan menahan dampak dari insiden siber.

c. Peningkatan kemampuan sektor dalam mendeteksi secara tepat waktu terjadinya peristiwa siber, yang ditempuh dengan:

   1) Menganalisis anomaly dan peristiwa siber; dan

   2) Memantau peristiwa siber berkelanjutan.

d. Peningkatan kemampuan sektor dalam mengambil tindakan terkait penanggulangan dan pemulihan insiden siber, yang ditempuh dengan:

   1) Menyusun perencanaan penanggulangan dan pemulihan insiden siber;

   2) Menganalisis dan melaporkan insiden siber;

   3) Meningkatkan keamanan setelah terjadinya insiden siber.

3.2 Sasaran penyelenggaraaan pelindungan infrastruktur informasi vital.
Sasaran penyelenggaraan pelindungan IIV merupakan arahan kepada penyelenggara IIV mengenai tujuan spesifik yang akan dicapai dalam memenuhi arah kebijakan yang terjadi diatas:

a. Penyelenggara IIV pada sektor pertahanan mampu menyusun strategi, kebijakan, dan prosedur pelindungan IIV;
b. Penyelenggara IIV pada sektor pertahanan mampu menilai dan mengelola risiko keamanan siber;
c. Penyelenggara IIV pada sektor pertahanan mampu mengelola risiko rantai pasok;
d. Penyelenggara IIV pada sektor pertahanan mampu melindungi aset fisik;
e. Penyelenggara IIV pada sektor pertahanan mampu melindungi data;
f. Penyelenggara IIV pada sektor pertahanan mampu melindungi sumber daya manusia.
g. Penyelenggara IIV pada sektor pertahanan mampu menganalisis anomali dan peristiwa siber;
h. Penyelenggara IIV pada sektor pertahanan mampu memantau peristiwa siber berkelanjutan;
i. Penyelenggara IIV pada sektor pertahanan menyusun perencanaan penanggulangan dan pemulihan insiden siber;

j. Penyelenggara IIV pada sektor pertahanan menganalisis dan melaporkan insiden siber;
k. Penyelenggara IIV pada sektor pertahanan meningkatkan keamanan setelah terjadinya insiden siber.

3.3 Target penerapan kontrol keamanan

Target penerapan kontrol keamanan sektor pertahanan merupakan nilai capaian yang bertujuan untuk memberikan gambaran kondisi penerapan keamanan siber pada penyelenggara IIV disektor pertahanan dihadapkan dengan sasaran penyelengga raan pada aspek domain identifikasi, proteksi, deteksi, dan penanggulan dan pemulihan.

Domain target penerapan kontrol keamanan sektor pertahanan ditentukan oleh Tingkat Kematangan Keamanan Siber. Pengukuran Tingkat Kematangan Siber dalam pelaksanaannya menghasilkan Katagori Tingkat Kematangan, terdiri atas:

a. level 1 (satu), dengan nilai kematangan pada rentang indeks 0 (nol) – 1,50 (satu koma lima nol) dinamakan level awal, dengan memiliki kriteria sebagai berikut:
   1) menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi awal;
   2) penerapan Keamanan Siber sudah memiliki prosedur yang terorganisir;
   3) penerapan Keamanan Siber bersifat informal;
   4) Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan; dan
   5) dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan

b. level 2 (dua), dengan dengan nilai kematangan pada rentang indeks 1,51 (satu koma lima satu) – 2,50 (dua koma lima nol) dinamakan level berulang, dengan memiliki kriteria sebagai berikut:
   1) menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang berulang;
   2) penerapan Keamanan Siber sudah memiliki prosedur yang terorganisir;
   3) penerapan Keamanan Siber bersifat informal;
   4) Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan; dan dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan

c. level 3 (tiga), dengan nilai kematangan pada rentang indeks 2,51 (dua koma lima satu) – 3,50 (tiga koma lima nol) dinamakan level terdefinisi, dengan memiliki kriteria sebagai berikut:
   1) menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terdefinisi dengan baik;
   2) penerapan Keamanan Siber telah terorganisir dengan jelas;
   3) penerapan Keamanan Siber bersifat formal;
   4) Keamanan Siber dilakukan secara berulang dan konsisten serta direviu secara berkala; dan
   5) dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan.

e. level 4 (empat), dengan nilai kematangan pada rentang indeks 3,51 (tiga koma lima satu) – 4,50 (empat koma lima nol) dinamakan level terkelola, dengan memiliki kriteria sebagai berikut:
   1) menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terkelola dengan baik;
   2) penerapan Keamanan Siber telah terorganisir dengan baik namun belum dilakukan proses otomatisasi;
   3) penerapan Keamanan Siber bersifat formal;
   4) Keamanan Siber dilakukan secara berulang dan implementasi perbaikan dilakukan berkelanjutan; dan
   5) dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan.

f. level 5 (lima), dengan nilai kematangan pada rentang indeks 4,51 (empat koma lima satu) – 5,0 (lima koma nol) dinamakan level inovatif, dengan memiliki kriteria sebagai berikut:
   1) menggambarkan kondisi penerapan Keamanan Siber telah diimplementasikan secara optimal;
   2) penerapan Keamanan Siber telah terorganisir dengan baik dan telah dilakukan proses otomatisasi;
   3) penerapan Keamanan Siber bersifat formal;
   4) keamanan siber dilakukan secara berulang dan konsisten serta telah terintegrasi;
   5) keamanan siber menjadi bagian budaya organisasi secara menyeluruh; dan
   6) dokumen manajemen risiko dan dokumen kontrol sudah ditetapkan.

BAB IV
RENCANA KERJA PENYELENGGARAAN PELINDUNGAN IIV SEKTOR PERTAHANAN

Rencana kerja penyelenggaraan pelindungan IIV sektor pertahanan pada tahun 2025 – 2029 dilaksanakan secara bertahap meliputi bidang identifikasi, proteksi, deteksi dan penanggulangan serta pemulihan dengan prioritas pada pelindungan tertentu.

1. Identifikasi.

   a. Menyusun strategi, kebijakan, dan prosedur pelindungan IIV;

      1) menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan Penyelenggara IIV.

      2) mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV

      3) menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan

      4) menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga

   b. Menilai dan mengelola risiko keamanan siber;

      1) Mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi

      2) Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal

      3) mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut;

      4) Menganalisa nilai risiko terhadap IIV

      5) Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko

      6) Menentukan dan mengomunikasikan toleransi risiko organisasi

      7) Mengelola hasil penerapan manajemen risiko yang telah ditetapkan

      8) Melakukan reviu hasil penerapan manajemen risiko

   c. Mengelola risiko rantai pasok.

      1) mengidentifikasikan dan menetapkan proses manajemen risiko rantai pasok.

      2) mengidentifikasikan pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV

      3) Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV

4) Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya

5) Menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut

2. Proteksi.

a. Melindungi aset fisik;

1) Melakukan penyediaan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV

2) memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur

3) memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur

4) memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman

5) memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman.

b. Melindungi data;

1) Melakukan pelindungan terhadap data yang tersimpan pada Penyelenggara IIV

2) Melakukan pelindungan terhadap data yang terkirim dari Penyelenggara IIV

3) memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai

4) Melakukan pengimplementasian pelindungan dari kebocoran data

5) Melakukan pengimplementasian mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data

6) memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala

7) Melakukan penyediaan kebijakan pemusnahan data.

c. Melindungi sumber daya manusia.

1) menerapkan prosedur pengelolaan keamanan terhadap personel

2) menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber

3) menyusun dan penerapan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di Penyelenggara IIV

3. Deteksi.

   a. Menganalisis anomali dan peristiwa siber;

      1) Menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data

      2) melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi

      3) Menentukan dampak dari Peristiwa Siber yang terdeteksi

      4) mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi

   b. Memantau peristiwa siber berkelanjutan.

      1) Menerapkan prosedur pendeteksi kode berbahaya dan tak berizin

      2) memonitor kegiatan personel yang berada di dalam lingkup sistem IIV

      3) memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV

      4) menerapkan teknologi pemindaian kerentanan terhadap sistem IIV

4. Penanggulangan dan pemulihan insiden siber.

   a. Menyusun perencanaan penanggulangan dan pemulihan insiden siber;

      1) Menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi

      2) Menyusunan dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi

      3) memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan ilaksanakan dan disimulasikan secara berkala

      4) memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan

      5) memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang

   b. Menganalisis dan melaporkan insiden siber;

      1) Mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal, maupun sumber informasi eksternal

      2) Mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber

      3) memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan

4) memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait

c. Meningkatkan keamanan setelah terjadinya insiden siber.

1) Meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan

2) Melakukan reviu dan/atau pembaharuan dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala

3) Mengumpulkan dan memelihara bukti hasil forensik digital

4) Meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala

Target waktu realisasi rencana kerja penyelenggaraan pelindungan IIV sektor pertahanan pada tahun 2025 – 2029 tertuang dalam bentuk matrik Peta Jalan Pelindungan IIV Sektor Pertahanan pada tabel IV.1.

TABEL IV.1 MATRIKS PETA JALAN PELINDUNGAN IIV SEKTOR PERTAHANAN TAHUN 2025 – 2029

Arah Kebijakan	Sasaran Penyelenggaraan	Target Penerapan	Rencana Kerja	Target dan Tahun Pencapaian (*)				
				2025	2026	2027	2028	2029
1	2	3	4	5	6	7	8	9
Peningkatan kemampuan sektor dalam mengidentifikasi konteks bisnis, sumber daya, dan risiko yang mendukung penyelenggaraan IIV di sektor pertahanan	Penyelenggara IIV pada sektor pertahanan mampu menyusun strategi, kebijakan, dan prosedur pelindungan IIV	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	Menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan penyelenggara IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Mengembangkan strategi untuk meningkatkan pelindungan terhadap IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Menetapkan persyaratan yang dibutuhkan untuk mendukung operasional IIV pada semua keadaan	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
	Penyelenggara IIV pada sektor pertahanan mampu menilai dan mengelola risiko keamanan siber	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	Mengidentifikasi dan mendokumentasikan kerentanan terhadap aset informasi.	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Mengidentifikasi potensi dampak terhadap layanan IIV dan kemungkinan terjadinya dampak tersebut	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Menganalisis nilai risiko terhadap IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko	level 2 (1,76 - 2,00	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Menentukan dan mengomunikasikan toleransi risiko organisasi	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			Mengelola hasil penerapan manajemen risiko yang telah ditetapkan	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
	Penyelenggara IIV pada sektor pertahanan mampu	Seluruh penyelenggara IIV pada sektor	Mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)

	mengelola risiko rantai pasok	pertahanan telah mencapai level 3	Mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)
			Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan keamanan siber pada Penyelenggara IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)
			Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)
			Menyiapkan rencana penanggulangan dan pemulihan pada layanan IIV dengan pihak ketiga yang mendukung layanan tersebut	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)
Peningkatan kemampuan sektor pertahanan dalam mencegah, membatasi, dan menahan dampak dari Insiden Siber;	melindungi aset fisik	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	menyediakan prosedur operasional pelindungan terhadap aset fisik yang mendukung layanan IIV	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan proses perbaikan dan pemeliharaan aset informasi pada layanan IIV dilakukan, dicatat, dan dikendalikan sesuai prosedur	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan IIV dilakukan dengan persetujuan penanggung jawab layanan IIV dan didokumentasikan sesuai prosedur	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan lingkungan fisik aset informasi pada layanan IIV dipantau secara berkala untuk mendeteksi potensi ancaman	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan prosedur dan penerapannya senantiasa ditinjau dan ditingkatkan sesuai perkembangan ancaman.	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
	melindungi data	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	pelindungan terhadap data yang tersimpan pada Penyelenggara IIV	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			pelindungan terhadap data yang terkirim dari Penyelenggara IIV	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan ketersediaan kapasitas ruang penyimpanan data yang memadai	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			mengimplementasikan pelindungan dari kebocoran data	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)

			mengimplementasikan mekanisme pengecekan integritas data untuk verifikasi perangkat lunak, perangkat keras, dan data	level 2 (2,01 - 2,25)	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)
			memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala	level 2 (2,01 - 2,25)	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)
			menyediakan kebijakan pemusnahan data	level 2 (2,01 - 2,25)	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)
	melindungi sumber daya manusia	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	menerapkan prosedur pengelolaan keamanan terhadap personel	level 2 (2,01 - 2,25)	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)
			menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber	level 2 (2,01 - 2,25)	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	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 (2,01 - 2,25)	level 2 (2,26 – 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)	level 3 (3,01 – 3,25)
peningkatan kemampuan sektor pertahanan dalam memantau secara tepat waktu terjadinya Peristiwa Siber;	menganalisis anomali dan Peristiwa Siber	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			menentukan dampak dari Peristiwa Siber yang terdeteksi	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
	memantau Peristiwa Siber berkelanjutan	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	Menerapkan prosedur pendeteksi kode berbahaya dan tak berizin	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			memonitor kegiatan personel yang berada di dalam lingkup sistem IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)
			menerapkan teknologi pemindaian kerentanan terhadap sistem IIV	level 2 (1,76 - 2,00)	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 – 2,75)	level 3 (2,76 – 3,00)

peningkatan kemampuan sektor pertahanan dalam mengambil tindakan terkait penanggulangan dan pemulihan Insiden Siber			menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan personel yang mengelola IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan personel yang mengelola IIV memahami prosedur penggunaan rekam cadang	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
	menganalisis dan melaporkan Insiden Siber	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	mengumpulkan informasi kondisi IIV terkini baik dari hasil deteksi internal, maupun sumber informasi eksternal	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
	meningkatkan keamanan setelah terjadinya Insiden Siber	Seluruh penyelenggara IIV pada sektor pertahanan telah mencapai level 3	meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			mengumpulkan dan memelihara bukti hasil forensik digital	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)
			meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala	level 2 (2,01 - 2,25)	level 2 (2,26 - 2,50)	level 3 (2,51 - 2,75)	level 3 (2,76 - 3,00)	level 3 (3,01 - 3,25)

BAB V
PENUTUP

Terlaksanakannya peta jalan yang telah disusun ini dapat diwujudkan melalui sinergi dan kolaborasi yang baik antara Kemhan selaku pengampu Sektor Pertahanan yang melakukan pengaturan, dan pengawasan pada Sektor Pertahanan dengan TNI, selaku unit organisasi Sektor Pertahanan.

Demikian, diharapkan melalui peta jalan ini, penyelenggaraan sistem elektronik IIV pada tahun 2025-2029 dapat berjalan sesuai dengan peraturan perundang-undangan dan memudahkan bagi Sektor Pertahanan.

MENTERI PERTAHANAN
REPUBLIK INDONESIA,

Cap/tertanda

SJAFRIE SJAMSOEDDIN

Autentikasi
Kepala Biro Tata Usaha dan Protokol
Setjen Kemhan

Charles Alling S.E., M.MDS.
Brigadir Jenderal TNI