KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA
BADAN INSTALASI STRATEGIS PERTAHANAN

PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN KEMENTERIAN PERTAHANAN NOMOR 02 TAHUN 2022

TENTANG

PEDOMAN PENILAIAN ANCAMAN SIBER TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA DI LINGKUNGAN KEMENTERIAN PERTAHANAN

DITETAPKAN DI JAKARTA
PADA TANGGAL 30 DESEMBER 2022

KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA
BADAN INSTALASI STRATEGIS PERTAHANAN

PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN
NOMOR 02 TAHUN 2022
TENTANG
PEDOMAN PENILAIAN ANCAMAN SIBER
TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA
DI LINGKUNGAN KEMENTERIAN PERTAHANAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN,

Menimbang :

a. bahwa untuk mengklasifikasikan level risiko ancaman siber terhadap pertahanan negara dari jenis, bentuk dan metodenya perlu pemilahan yang tepat untuk penilaian dalam penanganan pencegahan dan penanggulangan;
b. bahwa penilaian dalam penanganan pencegahan dan penanggulangan ancaman siber terhadap pertahanan negara diperlukan untuk mengetahui risiko, tingkat bahaya dan dampak ancaman siber;
c. bahwa untuk penilaian dalam penanganan pencegahan dan penanggulangan ancaman siber terhadap pertahanan negara di lingkungan Kementerian Pertahanan diperlukan pedoman sebagai acuan;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Kepala Badan Instalasi Strategis Pertahanan Kementerian Pertahanan tentang Pedoman Penilaian Ancaman Siber Terhadap Penyelenggaraan Pertahanan Negara di Lingkungan Kementerian Pertahanan;

Mengingat :

1. Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber (Berita Negara Republik Indonesia Tahun 2014 Nomor 1712);
2. Peraturan Menteri Pertahanan Nomor 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan (Berita Negara Republik Indonesia Tahun 2019 Nomor 314);

3. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488);

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN KEMENTERIAN PERTAHANAN TENTANG PEDOMAN PENILAIAN ANCAMAN SIBER TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA DI LINGKUNGAN KEMENTERIAN PERTAHANAN.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Kepala Badan ini yang dimaksud dengan:

1. Penilaian adalah proses, cara, dan/atau perbuatan untuk memberikan nilai.
2. Ancaman Siber adalah segala upaya, kegiatan, dan/atau tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat melemahkan, merugikan dan/atau menghancurkan infrastruktur informasi vital, sistem elektronik, data dan informasi Kementerian Pertahanan.
3. Kementerian Pertahanan yang selanjutnya disebut Kemhan adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
4. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
5. Badan Instalasi Strategis Pertahanan Kemhan yang selanjutnya disebut Bainstrahan Kemhan adalah badan yang mempunyai tugas melaksanakan pengelolaan instalasi strategis, pertahanan siber dan informasi pertahanan.
6. Kepala Bainstrahan Kemhan yang selanjutnya disebut Kabainstrahan Kemhan adalah kepala badan yang mempunyai tugas melaksanakan pengelolaan instalasi strategis, pertahanan siber dan informasi pertahanan.
7. Pusat Pertahanan Siber yang selanjutnya disebut Pushansiber adalah unsur pelaksana tugas dan fungsi Bainstrahan Kemhan.
8. Kepala Pushansiber yang selanjutnya disebut Kapushansiber adalah kepala pusat yang melaksanakan tugas dan fungsi Bainstrahan Kemhan di bidang tata kelola, kerja sama, operasi, dan jaminan keamanan pertahanan siber.

Pasal 2

Peraturan Kepala Badan ini disusun dengan maksud sebagai pedoman dalam Penilaian Ancaman Siber terhadap penyelenggaraan pertahanan negara.

Pasal 3

Penilaian Ancaman Siber bertujuan untuk menentukan klasifikasi tingkat risiko Ancaman Siber di lingkungan Kemhan

Pasal 4

Fungsi Penilaian Ancaman Siber untuk mengetahui risiko, tingkat bahaya dan dampak dari Ancaman Siber.

Pasal 5

Penilaian Ancaman Siber dilakukan dengan memperhatikan:

a. frekuensi pelaksanaan *vulnerability assessment* dengan menyesuaikan pada tingkat kerentanan sistem dan risiko yang dihadapi dari hasil proses identifikasi Ancaman Siber;
b. analisis atas ancaman dan kerentanan serta melakukan klasifikasi ancaman dan kerentanan berdasarkan potensi dampak yang dapat ditimbulkan;
c. pemantauan terhadap perkembangan Ancaman Siber yang terkini (*emerging cyber threat*), baik dari sisi teknologi, taktik dan teknik serangan, serta prosedur atau pola serangan;
d. inventaris risiko (*risk repository*) sesuai dengan hasil pemantauan yang diperbaharui secara berkala; dan
e. penilaian ancaman dan kerentanan sebelum menerapkan pembaharuan teknologi, produk, layanan yang dapat mempengaruhi risiko keamanan siber.

BAB II

PEDOMAN PENILAIAN ANCAMAN SIBER

Bagian Kesatu

Pedoman Penilaian

Pasal 6

Pedoman Penilaian Ancaman Siber digunakan sebagai dasar untuk melaksanakan dan menentukan klasifikasi Ancaman Siber.

Pasal 7

(1) Pedoman Penilaian Ancaman Siber sebagaimana dimaksud dalam Pasal 6 menggunakan standar sebagai berikut:
    a. *international standardization organization* (ISO) 27000 *series*;
    b. *national institute of standards and technology* (NIST) *cybersecurity framework*;
    c. *open web application security project* (OWASP);
    d. *information technology infrastructure library* (ITIL); dan
    e. standar Penilaian Ancaman Siber lainnya sesuai kebutuhan.

(2) *International standardization organization* (ISO) 27000 *series* sebagaimana dimaksud pada ayat (1) huruf a merupakan suatu standar internasional dalam

menerapkan sistem manajemen kemanan informasi atau lebih dikenal dengan *information security management systems* (ISMS).

(3) *National institute of standards and technology* (NIST) *cybersecurity framework* sebagaimana dimaksud pada ayat (1) huruf b menyediakan mekanisme Penilaian untuk menentukan kemampuan *cyber security* saat ini, menetapkan sasaran individual, dan membuat rencana untuk memperbaiki serta memelihara program *cybersecurity*.

(4) *Open web application security project* (OWASP) sebagaimana dimaksud pada ayat (1) huruf c merupakan sebuah organisasi nirlaba yang berlaku sebagai salah satu standar pengujian kerentanan keamanan aplikasi.

(5) *Information technology infrastructure library* (ITIL) sebagaimana dimaksud pada ayat (1) huruf d bertujuan untuk menentukan pedoman penyediaan layanan teknologi informasi yang tepat dan efisien dalam organisasi.

(6) Standar Penilaian Ancaman Siber lainnya sesuai kebutuhan sebagaimana dimaksud pada ayat (1) huruf e merupakan standar Penilaian Ancaman Siber yang diakui secara internasional.

Bagian Kedua
Klasifikasi Penilaian

Pasal 8

Klasifikasi Penilaian Ancaman Siber dilaksanakan melalui tahapan sebagai berikut:

a. identifikasi risiko;
b. analisis risiko; dan
c. evaluasi risiko.

Pasal 9

(1) Identifikasi risiko sebagaimana dimaksud dalam Pasal 8 huruf a dilakukan untuk menemukan, menginventarisir dan menggolongkan unsur risiko sekaligus untuk mendapatkan informasi tentang bagaimana, dimana, dan mengapa risiko tersebut dapat terjadi.

(2) Identifikasi risiko sebagaimana dimaksud pada ayat (1) dilaksanakan dengan proses sebagai berikut:
   a. identifikasi aset;
   b. identifikasi ancaman;
   c. identifikasi kerentanan; dan
   d. identifikasi dampak.

(3) Identifikasi aset sebagaimana dimaksud pada ayat (2) huruf a dilaksanakan dengan cara pengidentifikasian dan penggolongan aset yang dimiliki.

(4) Identifikasi ancaman sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan cara mendaftarkan seluruh jenis Ancaman Siber yang terjadi, baik ancaman yang berasal dari internal maupun eksternal.

(5) Identifikasi kerentanan sebagaimana dimaksud pada ayat (2) huruf c dilaksanakan untuk mengetahui seluruh kerentanan yang dimiliki dengan cara membuat daftar seluruh kerentanan sistem yang mungkin dieksploitasi oleh ancaman yang telah terindentifikasi.

(6) Kerentanan sebagaimana dimaksud pada ayat (5) ditinjau dari segi organisasi, personel, lokasi, perangkat keras dan perangkat lunak.

(7) Identifikasi dampak sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan cara mengidentifikasi kerugian yang akan dialami.

(8) Hasil identifikasi dampak sebagaimana dimaksud pada ayat (7) diuraikan pada tahap analisis risiko sebagai bahan pertimbangan dalam membuat kebijakan terkait proses pengamanan informasi dalam organisasi.

(9) Kegiatan identifikasi risiko sebagaimana dimaksud pada ayat (1) sampai dengan ayat (8) dilakukan oleh Pranata Komputer Ahli Pertama.

(10) Pranata Komputer Ahli Pertama sebagaimana dimaksud pada ayat (9) melaporkan hasil kegiatan identifikasi risiko kepada Kepala Sub Bidang Pemantauan, Analisis dan Pelaporan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan, Kepala Subbidang Penindakan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan dan Kepala Subbidang Digital Forensik dan Pemulihan Bidang Operasi Siber Pushansiber Bainstrahan Kemhan untuk diputuskan oleh Kepala Bidang Operasi Siber Pushansiber Bainstrahan Kemhan.

Pasal 10

(1) Analisis risiko sebagaimana dimaksud dalam Pasal 8 huruf b merupakan kegiatan mengamati aktivitas Ancaman Siber yang berpotensi menimbulkan risiko.

(2) Analisis risiko sebagaimana dimaksud pada ayat (1) dilakukan dengan cara sebagai berikut:
   a. analisis tingkat kemungkinan risiko;
   b. analisis dampak risiko; dan
   c. penentuan skala risiko.

(3) Analisis tingkat kemungkinan risiko sebagaimana dimaksud pada ayat (2) huruf a dilaksanakan dengan melakukan estimasi peluang terjadinya risiko Ancaman Siber.

(4) Analisis dampak risiko sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan melakukan estimasi tingkat dampak yang akan diterima akibat terjadinya Ancaman Siber.

(5) Penentuan skala risiko sebagaimana dimaksud pada ayat (2) huruf c dilaksanakan dengan cara mengkombinasikan tingkat kemungkinan risiko dan dampak risiko.

(6) Berdasarkan analisis risiko sebagaimana dimaksud pada ayat (2) didapatkan hasil analisis risiko.

(7) Kegiatan analisis risiko sebagaimana dimaksud pada ayat (1) sampai dengan ayat (6) yang dilakukan oleh

Pranata Komputer Ahli Pertama.

(8) Pranata Komputer Ahli Pertama sebagaimana dimaksud pada ayat (7) melaporkan hasil analisis risiko kepada Kepala Subbidang Keamanan Infrastruktur dan Komunikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan dan Kepala Subbidang Keamanan Aplikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan untuk diputuskan oleh Kepala Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan.

Pasal 11

(1) Evaluasi risiko sebagaimana dimaksud dalam Pasal 8 huruf c merupakan kegiatan yang dilaksanakan dengan menentukan level risiko dan prioritas risiko.

(2) Penentuan level risiko sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. tingkat rendah;
   b. tingkat sedang; dan
   c. tingkat tinggi.

(3) Level risiko tingkat rendah sebagaimana dimaksud pada ayat (2) huruf a ditentukan dari skala risiko 0 (nol) sampai dengan 2 (dua).

(4) Level risiko tingkat sedang sebagaimana dimaksud pada ayat (2) huruf b ditentukan dari skala risiko 3 (tiga) sampai dengan 5 (lima).

(5) Level risiko tingkat tinggi sebagaimana dimaksud pada ayat (2) huruf c ditentukan dari skala risiko 6 (enam) sampai dengan 8 (delapan).

(6) Level risiko sebagaimana dimaksud pada ayat (1) ditentukan dari hasil skala risiko.

(7) Penentuan prioritas risiko sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan kemungkinan risiko, dampak risiko dan skala risiko.

(8) Skala risiko tertinggi mendapat prioritas paling tinggi.

(9) Apabila terdapat lebih dari satu risiko yang memiliki skala risiko yang sama maka prioritas risiko ditentukan berdasarkan urutan kemungkinan risiko dari tertinggi hingga terendah.

(10) Apabila masih terdapat lebih dari satu risiko yang memiliki skala risiko dan kemungkinan risiko yang sama maka prioritas risiko ditentukan berdasarkan urutan dampak risiko dari yang tertinggi hingga terendah.

(11) Apabila masih terdapat lebih dari satu risiko yang memiliki skala risiko, kemungkinan risiko dan dampak risiko yang sama, maka prioritas risiko ditentukan berdasarkan kebijakan pimpinan dalam mengelola risiko tersebut.

(12) Ketentuan mengenai contoh hasil penentuan prioritas risiko tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Kepala Badan ini.

Pasal 12

(1) Evaluasi risiko sebagaimana dimaksud dalam Pasal 11 dilakukan oleh Pranata Komputer Ahli Pertama.
(2) Pranata Komputer Ahli Pertama sebagaimana dimaksud pada ayat (1) melaporkan hasil evaluasi risiko kepada Kepala Subbidang Keamanan Infrastruktur dan Komunikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan, Kepala Subbidang Keamanan Aplikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan untuk diputuskan oleh Kepala Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan.

Bagian Ketiga
Hasil Penilaian

Pasal 13

(1) Hasil Penilaian Ancaman Siber dijadikan dasar penetapan Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan.
(2) Hasil penilaian Ancaman Siber sebagaimana dimaksud pada ayat (1) dilaporkan kepada Kapushansiber Bainstrahan Kemhan.

BAB III
WEWENANG DAN TANGGUNG JAWAB

Pasal 14

(1) Wewenang dan tanggung jawab dalam penilaian Ancaman Siber dilaksanakan oleh Tim Penilai.
(2) Tim penilai sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. Kepala Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan;
    b. Kepala Subbidang Keamanan Infrastruktur dan Komunikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan;
    c. Kepala Subbidang Keamanan Aplikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan; dan
    d. Pranata Komputer Ahli Pertama.

Pasal 15

(1) Kepala Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a mempunyai tugas melaksanakan penyiapan penjaminan keamanan pertahanan siber dari ancaman eksternal.
(2) Kepala Subbidang Keamanan Infrastruktur dan Komunikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b mempunyai tugas melakukan penyiapan bahan penyusunan kebijakan teknis, pelaksanaan, pemantauan, evaluasi

dan pelaporan di bidang keamanan infrastruktur dan komunikasi meliputi pengujian, analisis, dan rekomendasi keamanan infrastruktur dan komunikasi.

(3) Kepala Subbidang Keamanan Aplikasi Bidang Penjaminan Keamanan Pushansiber Bainstrahan Kemhan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c mempunyai tugas melakukan penyiapan bahan penyusunan kebijakan teknis, pelaksanaan, pemantauan, evaluasi dan pelaporan di bidang keamanan aplikasi meliputi pengujian, analisis, dan rekomendasi keamanan aplikasi.

(4) Pranata Komputer Ahli Pertama sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf d mempunyai tugas merencanakan, menganalisis, merancang, mengimplementasikan, mengembangkan dan atau mengoperasikan sistem informasi berbasis komputer.

BAB IV
PENGENDALIAN DAN PENGAWASAN

Pasal 16

Pengendalian Penilaian Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan dilaksanakan oleh Kabainstrahan Kemhan.

Pasal 17

Pengawasan Penilaian Ancaman Siber terhadap penyelenggaraan pertahanan negara di lingkungan Kemhan dilaksanakan oleh Kapushansiber Bainstrahan Kemhan.

BAB V
KETENTUAN PENUTUP

Pasal 18

Peraturan Kepala Badan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 30 Desember 2022

KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN,

YUDI ABRIMANTYO, S.I.P., M.Sc.
MAYOR JENDERAL TNI

LAMPIRAN
PERATURAN KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN
NOMOR 02 TAHUN 2022
TENTANG
PEDOMAN PENILAIAN ANCAMAN SIBER TERHADAP PENYELENGGARAAN PERTAHANAN NEGARA DI LINGKUNGAN KEMENTERIAN PERTAHANAN

TABEL HASIL PENENTUAN PRIORITAS RISIKO

Prioritas Risiko	Skala Risiko	Kemungkinan Risiko	Dampak Risiko	Risiko
1	5	4	3	Serangan *Malware/ Virus*
2	5	3	4	Serangan *Worm Stuxnet*
	5	3	4	Serangan *Ransomware WannaCry*
3	4	3	3	Serangan *SQL Injection*
4	4	4	2	Serangan *Spam*
5	3	3	2	*Network Intrusion*
	3	3	2	Serangan *Distributed Denial of Service* (DDoS)
6	2	3	1	Serangan *Defacement*
	2	3	1	Penyusupan Siber
7	1	2	1	Kegiatan *Jamming*

KEPALA BADAN INSTALASI STRATEGIS PERTAHANAN
KEMENTERIAN PERTAHANAN,

YUDI ABRIMANTYO, S.I.P., M.Sc.
MAYOR JENDERAL TNI