PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 5 TAHUN 2024
TENTANG
RENCANA AKSI NASIONAL KEAMANAN SIBER
TAHUN 2024-2028

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 15 ayat (7) Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Rencana Aksi Nasional Keamanan Siber Tahun 2024-2028;

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 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);
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);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG RENCANA AKSI NASIONAL KEAMANAN SIBER TAHUN 2024-2028.

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. 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.

2. Rencana Aksi Nasional Keamanan Siber yang selanjutnya disebut RAN Kamsiber adalah rencana aksi tingkat nasional yang berisi upaya terencana dan terukur untuk menjabarkan dan mengimplementasikan fokus area strategi Keamanan Siber nasional.
3. Instansi Penyelenggara Negara adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan.
4. Pemangku Kepentingan adalah para pihak yang memiliki peran dalam penerapan strategi Keamanan Siber nasional.
5. Badan Siber dan Sandi Negara yang selanjutnya disebut Badan adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan sandi.

Pasal 2

(1) RAN Kamsiber berlaku untuk tahun 2024 sampai dengan tahun 2028.
(2) RAN Kamsiber merupakan bagian dari strategi Keamanan Siber nasional sesuai dengan ketentuan peraturan perundang-undangan.
(3) RAN Kamsiber sebagaimana dimaksud pada ayat (1) memuat:
    a. arah kebijakan;
    b. tantangan;
    c. sasaran strategis;
    d. kegiatan;
    e. indikator keberhasilan;
    f. target dan tahun capaian;
    g. penanggung jawab; dan
    h. instansi terkait.
(4) RAN Kamsiber sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 3

Dalam hal terdapat perubahan rencana pembangunan nasional, perkembangan ilmu pengetahuan dan teknologi, dan perkembangan lingkungan strategis, dapat dilakukan peninjauan kembali terhadap RAN Kamsiber sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 4

(1) RAN Kamsiber wajib dilaksanakan oleh Instansi Penyelenggara Negara sesuai dengan tugas dan fungsi masing-masing.
(2) Dalam melaksanakan RAN Kamsiber sebagaimana dimaksud pada ayat (1), Instansi Penyelenggara Negara dapat mengikutsertakan Pemangku Kepentingan.
(3) Pemangku Kepentingan sebagaimana dimaksud ayat (2) meliputi:
    a. pelaku usaha;
    b. akademisi; dan

c. komunitas.

Pasal 5

Dalam pelaksanaan RAN Kamsiber, Badan bertanggung jawab:
a. mengoordinasikan pelaksanaan RAN Kamsiber;
b. memantau pelaksanaan RAN Kamsiber;
c. mengevaluasi pelaksanaan RAN Kamsiber; dan
d. melaporkan hasil pelaksanaan RAN Kamsiber.

Pasal 6

Dalam rangka mengoordinasikan pelaksanaan RAN Kamsiber sebagaimana dimaksud dalam Pasal 5 huruf a, Badan melakukan:
a. pemberian asistensi;
b. kerja sama dengan berbagai pihak;
c. rapat koordinasi paling sedikit 6 (enam) bulan sekali; dan/atau
d. bentuk kegiatan lainnya yang mendukung pelaksanaan RAN Kamsiber.

Pasal 7

Dalam rangka memantau pelaksanaan RAN Kamsiber sebagaimana dimaksud dalam Pasal 5 huruf b, Badan melakukan:
a. pemantauan capaian kegiatan;
b. pemberian rekomendasi atas kendala; dan/atau
c. bentuk kegiatan lainnya yang mendukung pemantauan pelaksanaan RAN Kamsiber.

Pasal 8

(1) Dalam rangka mengevaluasi pelaksanaan RAN Kamsiber sebagaimana dimaksud dalam Pasal 5 huruf c, Badan melakukan:
    a. penyelenggaraan evaluasi capaian pelaksanaan RAN Kamsiber; dan/atau
    b. bentuk kegiatan lainnya yang mendukung evaluasi pelaksanaan RAN Kamsiber.
(2) Badan melakukan evaluasi pelaksanaan RAN Kamsiber sebagaimana dimaksud pada ayat (1) paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(3) Dalam pelaksanaan evaluasi sebagaimana dimaksud pada ayat (2), Badan dapat mengikutsertakan Instansi Penyelenggara Negara sebagai Penanggung Jawab kegiatan RAN Kamsiber.
(4) Hasil evaluasi sebagaimana dimaksud pada ayat (1) digunakan sebagai bahan pertimbangan dalam penilaian efektivitas pencapaian RAN Kamsiber.

Pasal 9

(1) Dalam rangka memantau dan mengevaluasi sebagaimana dimaksud dalam Pasal 7 dan Pasal 8, Instansi Penyelenggara Negara sebagai Penanggung Jawab kegiatan RAN Kamsiber wajib menyampaikan perkembangan capaian pelaksanaan RAN Kamsiber kepada Badan secara berkala setiap 6 (enam) bulan sekali,

paling lambat tanggal 30 Juni dan 31 Desember tahun anggaran berjalan.

(2) Badan menghimpun capaian perkembangan pelaksanaan RAN Kamsiber sebagaimana dimaksud pada ayat (1) sebagai bahan perumusan dan penyiapan laporan pelaksanaan RAN Kamsiber kepada Presiden.

Pasal 10

(1) Dalam rangka melaporkan hasil pelaksanaan RAN Kamsiber sebagaimana dimaksud dalam Pasal 5 huruf d, Badan melakukan:
   a. publikasi hasil pelaksanaan RAN Kamsiber; dan/atau
   b. bentuk kegiatan lainnya yang mendukung pelaporan pelaksanaan RAN Kamsiber.

(2) Kepala Badan melaporkan hasil pelaksanaan RAN Kamsiber sebagaimana dimaksud pada ayat (1) kepada Presiden secara berkala setiap 1 (satu) tahun sekali atau sewaktu-waktu apabila diperlukan.

Pasal 11

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 7 Juni 2024

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 10 Juni 2024

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

#KUMHAMPASTI
Ditandatangani secara elektronik oleh :

ASEP N. MULYANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2024 NOMOR 314

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 5 TAHUN 2024
TENTANG
RENCANA AKSI NASIONAL KEAMANAN SIBER
TAHUN 2024-2028

# RENCANA AKSI NASIONAL KEAMANAN SIBER TAHUN 2024-2028

## BAB I
## ARAH KEBIJAKAN

### A. LATAR BELAKANG

Kondisi Keamanan Siber global saat ini menjadi suatu isu yang semakin mendesak seiring dengan berkembangnya teknologi informasi dan komunikasi. Ancaman siber yang beragam seperti peretasan, pencurian data, dan ancaman siber lainnya, telah menarik perhatian global. Tren ini menunjukkan peningkatan frekuensi, kompleksitas, dan dampak serangan siber terhadap sistem informasi, infrastruktur kritis, dan privasi individu. Oleh karena itu, Keamanan Siber menjadi sebuah prioritas yang tak dapat diabaikan.

Dalam rangka menjawab tantangan Keamanan Siber ini, pemerintah telah menerbitkan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber sebagai amanat dari Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Penyelenggaraan strategi Keamanan Siber nasional merupakan langkah konkret untuk menghadapi ancaman siber yang semakin kompleks, dan untuk mencapai efektivitas penyelenggaraannya perlu penjabaran dalam bentuk RAN Kamsiber.

Dalam penyusunan RAN Kamsiber, perlu memperhatikan rencana pembangunan nasional, perkembangan ilmu pengetahuan dan teknologi, dan perkembangan lingkungan strategis. Ketiganya merupakan pilar penting dalam memberikan arah kebijakan dan sasaran strategi RAN Kamsiber sehingga RAN Kamsiber menjadi lebih kontekstual dan relevan terhadap kebutuhan nasional dalam jangka panjang.

Mengingat pendekatan aktor dalam strategi Keamanan Siber nasional adalah *multi-stakeholder* yang direpresentasikan oleh *quadhelix stakeholder*, yaitu Instansi Penyelenggara Negara, pelaku usaha, akademisi, dan komunitas, maka RAN Kamsiber harus dirumuskan berdasarkan komitmen dan berkolaborasi dengan seluruh *quadhelix stakeholder* tersebut.

RAN Kamsiber digunakan untuk memberikan acuan bagi Instansi Penyelenggara Negara dengan melibatkan pelaku usaha, akademisi, dan

komunitas dalam mengimplementasikan dan memastikan efektivitas 8 (delapan) fokus area strategi Keamanan Siber nasional yang mencakup tata kelola, manajemen risiko, kesiapsiagaan dan ketahanan, penguatan pelindungan infrastruktur informasi vital, kemandirian kriptografi nasional, peningkatan kapabilitas, kapasitas, dan kualitas, kebijakan Keamanan Siber, dan kerja sama internasional. Strategi yang terkandung dalam RAN Kamsiber memerinci langkah-langkah konkret setiap fokus area melalui penjabaran kegiatan yang terarah dan terukur. Adapun RAN Kamsiber tersebut disusun dalam bentuk matriks yang memuat tantangan, sasaran strategis, kegiatan, indikator keberhasilan, target dan tahun capaian, penanggung jawab, dan instansi terkait.

Untuk memastikan efektivitas pelaksanaan RAN Kamsiber, Badan dengan Instansi Penyelenggara Negara melakukan pemantauan dan evaluasi capaian RAN Kamsiber, yang hasil pelaksanaannya dilaporkan oleh Kepala Badan kepada Presiden setiap 1 (satu) tahun sekali atau sewaktu-waktu apabila diperlukan.

## B. ARAH KEBIJAKAN DAN SASARAN STRATEGI KEAMANAN SIBER NASIONAL

Amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa negara akan melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia dan untuk memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial. Hal ini menunjukkan tingginya komitmen untuk mewujudkan cita-cita bangsa Indonesia salah satunya melalui penguatan pertahanan dan keamanan negara yang andal dan berdaya saing guna mewujudkan kesejahteraan masyarakat.

Tindakan tegas yang merupakan upaya preventif perlu dibangun dalam RAN Kamsiber dengan mengakomodasi dan memberdayakan seluruh aspek Keamanan Siber pada Instansi Penyelenggara Negara dengan melibatkan pelaku usaha, akademisi, dan komunitas pada tingkat nasional maupun global, termasuk melalui kerja sama internasional, berdasarkan prinsip kesemestaan dari seluruh komponen bangsa. Dalam praktiknya, upaya mewujudkan Keamanan Siber nasional akan berjalan beriringan dengan upaya bangsa dalam membangun kekuatan dan kapabilitas siber nasional yang kompetitif serta berdaya tangkal di tingkat global.

Pasal 30 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 menyatakan bahwa tiap-tiap warga negara berhak dan wajib ikut serta dalam usaha pertahanan dan keamanan negara. Keamanan Siber merupakan bagian dari pertahanan dan keamanan negara yang tidak hanya menjadi hak dan kewajiban aparatur negara, melainkan juga hak dan kewajiban setiap warga negara dalam hal ini sebagai Pemangku Kepentingan untuk ikut serta berperan dalam mendukung Keamanan Siber.

Dalam Rencana Pembangunan Jangka Menengah Nasional Tahun 2019-2024, penguatan ketahanan dan Keamanan Siber masuk menjadi agenda kegiatan prioritas dalam rangka strategi menjaga stabilitas keamanan nasional. Adapun proyek prioritas yang diagendakan dalam Rencana Pembangunan Jangka Menengah Nasional Tahun 2019-2024 untuk mewujudkan penguatan ketahanan dan Keamanan Siber, yaitu:

1) pembangunan dan penguatan tim cepat tanggap Keamanan Siber;
2) penguatan infrastruktur, sumber daya manusia, dan regulasi Keamanan Siber;
3) pencegahan kejahatan siber dan peningkatan kerja sama internasional bidang siber; dan
4) penyelesaian kejahatan siber.


Gambar Arah kebijakan dan Sasaran Strategis Keamanan Siber pada Rencana Pembangunan Jangka Menengah Nasional Tahun 2019-2024

Di samping itu, Presiden dalam beberapa kali kesempatan telah memberikan arahan untuk melakukan percepatan transformasi digital dengan 3 (tiga) fokus kebijakan yaitu kesetaraan akses digital, literasi digital, dan ekosistem digital yang aman. Pada konteks ekosistem digital yang aman, saat ini kebocoran data, penyalahgunaan di ranah digital, dan kejahatan siber dapat berpotensi menimbulkan kerugian ekonomi hingga USD 5 Triliun pada tahun 2024. Oleh karena itu, diperlukan langkah-langkah strategis dan akseleratif dalam penyelenggaraan Keamanan Siber dengan tetap memperhatikan prinsip-prinsip pelindungan data pribadi sesuai ketentuan peraturan perundang-undangan.

Arahan Presiden lebih lanjut terkait transformasi digital yang perlu diinternalisasi dalam strategi Keamanan Siber nasional, sebagai berikut:

1) percepatan perluasan akses dan peningkatan infrastruktur digital yang diikuti percepatan penyediaan layanan internet di 12.500 desa atau kelurahan dan titik layanan publik;
2) *roadmap* transformasi digital di sektor-sektor strategis seperti: pemerintahan, layanan publik, bantuan sosial, sektor pendidikan, sektor kesehatan, perdagangan, sektor industri, dan sektor penyiaran;
3) percepatan integrasi pusat data nasional;
4) mempersiapkan kebutuhan sumber daya manusia talenta digital;
5) mempersiapkan dengan cepat regulasi, skema pendanaan, dan pembiayaan transformasi digital.

## C. FOKUS AREA STRATEGI KEAMANAN SIBER NASIONAL

Untuk melanjutkan Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024 dan sesuai dengan Arahan Presiden mengenai penguatan Keamanan Siber sebagai pondasi transformasi digital, maka arah kebijakan Keamanan Siber nasional difokuskan pada:

1) Tata kelola
   a. penguatan ekosistem Keamanan Siber mencakup sumber daya manusia, proses, dan teknologi; dan
   b. peningkatan sinergi dan kolaborasi dalam pelaksanaan Keamanan Siber.
2) Manajemen risiko
   a. pengoptimalan identifikasi risiko, analisis risiko, dan tindak lindung risiko Keamanan Siber;
   b. peningkatan efektivitas mitigasi risiko Keamanan Siber nasional;
   c. peningkatan sinergi dan kolaborasi para Pemangku Kepentingan; dan

d. peningkatan kualitas penyusunan dan implementasi kebijakan Keamanan Siber berbasis risiko.

3) Kesiapsiagaan dan ketahanan
   a. pembangunan kapabilitas tanggap insiden siber yang efektif dan efisien;
   b. perumusan dan penetapan rencana kontingensi untuk pengelolaan krisis siber;
   c. penyelenggaraan penanganan tanggap darurat; dan
   d. penguatan pertukaran informasi yang aman dan memiliki waktu akses yang tinggi.
4) Penguatan pelindungan infrastruktur informasi vital
   a. penyelenggaraan pelindungan infrastruktur informasi vital; dan
   b. peningkatan pembinaan dan pengawasan penyelenggaraan pelindungan infrastruktur informasi vital.
5) Kemandirian kriptografi nasional
   a. penetapan kebijakan kriptografi nasional;
   b. peningkatan riset, pengembangan, dan inovasi di bidang kriptografi untuk mendukung pembangunan nasional;
   c. penerapan kebijakan kriptografi nasional pada Pemangku Kepentingan; dan
   d. pembangunan dan pengembangan industri kriptografi nasional.
6) Peningkatan kapabilitas, kapasitas, dan kualitas
   a. pengembangan kurikulum berkaitan dengan Keamanan Siber pada pendidikan anak usia dini, pendidikan dasar, pendidikan menengah, dan pendidikan tinggi;
   b. pengembangan dan penerapan program keterampilan dan pelatihan sumber daya manusia;
   c. pengembangan dan penerapan program peningkatan kesadaran Keamanan Siber yang terkoordinasi dan berkesinambungan;
   d. penguatan kapasitas teknologi Keamanan Siber;
   e. peningkatan riset, pengembangan, dan inovasi ilmu pengetahuan dan teknologi di bidang Keamanan Siber; dan
   f. pengembangan program yang khusus untuk sektor dan kelompok rentan sesuai dengan kebutuhan.
7) Kebijakan Keamanan Siber
   a. analisis dan evaluasi terhadap kebijakan Keamanan Siber;
   b. perumusan dan pemberian rekomendasi kebijakan di bidang Keamanan Siber;

c. pembudayaan hukum dan peningkatan kesadaran hukum masyarakat; dan
d. penegakan hukum di bidang Keamanan Siber secara terpadu.

8) Kerja sama internasional
a. penetapan kebijakan dan prioritas kerja sama internasional di bidang Keamanan Siber;
b. peningkatan inisiatif kerja sama internasional dalam rangka mendukung terciptanya ruang siber yang aman, damai, dan terbuka serta meningkatkan kapasitas nasional di bidang Keamanan Siber;
c. peningkatan kerja sama praktis, berbagi informasi, dan praktik terbaik dalam menghadapi krisis siber; dan
d. peningkatan peran Indonesia dalam forum bilateral, regional, dan multilateral di bidang Keamanan Siber.

RAN Kamsiber telah disusun dalam bentuk matriks yang memuat tantangan, sasaran strategis, kegiatan, indikator keberhasilan, target dan tahun capaian, penanggung jawab, dan instansi terkait diuraikan lebih lanjut pada BAB II.

BAB II
MATRIKS RENCANA AKSI NASIONAL KEAMANAN SIBER TAHUN 2024-2028

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| **Fokus Area 1 : Tata Kelola** | | | | | | | | | | |
| 1.1. Penguatan ekosistem Keamanan Siber mencakup sumber daya manusia, proses, dan teknologi | | | | | | | | | | |
| 1. Usaha pemerintah menghadirkan standar nasional pada semua sektor dalam penguatan ekosistem Keamanan Siber belum maksimal di tengah banyaknya standar internasional Keamanan Siber | Tersedianya kriteria dan standar bidang Keamanan Siber yang diadopsi Pemangku Kepentingan | 1. Menyusun kriteria dan standar Keamanan Siber nasional termasuk mengidentifikasi, menganalisis, maupun mengoordinasikan instansi terkait mengenai standar Keamanan Siber yang sesuai untuk industri terkait | Tersedianya Standar Kompetensi Kerja Nasional Indonesia di bidang Keamanan Siber dan Sandi | 1 Dokumen | 1 Dokumen | 1 Dokumen | 1 Dokumen | - | Badan Siber dan Sandi Negara | Badan Nasional Sertifikasi Profesi; Kementerian Ketenagakerjaan |
| | | | Tersedianya Standar Nasional Indonesia di bidang Keamanan Informasi dan Keamanan Siber | 10 Dokumen | 10 Dokumen | 10 Dokumen | 10 Dokumen | 10 Dokumen | Badan Siber dan Sandi Negara | Badan Standardisasi Nasional |
| | | | Tersedianya skema penilaian kesesuaian teknologi Keamanan Siber dan sandi | - | 1 Dokumen | - | - | - | Badan Siber dan Sandi Negara | Badan Standardisasi Nasional |
| 1.2. Peningkatan sinergi dan kolaborasi dalam pelaksanaan Keamanan Siber | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Koordinasi para Pemangku Kepentingan terkait Keamanan Siber masih lemah<br><br>2. Penyelenggaraan Keamanan Siber para Pemangku Kepentingan masih berjalan parsial | Terkoordinasinya penyelenggaraan Keamanan Siber para Pemangku Kepentingan | 1. Menyelenggarakan forum koordinasi sektoral bidang Keamanan Siber | Terselengggaranya forum koordinasi sektoral | 7 Forum | 8 Forum | 8 Forum | 10 Forum | 10 Forum | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 2. Menyelenggarakan koordinasi dalam penyusunan arsitektur Sistem Pemerintahan Berbasis Elektronik, domain keamanan Sistem Pemerintahan Berbasis Elektronik, dan kebijakan internal manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik di setiap Instansi Penyelenggara Negara | Tersedianya arsitektur Sistem Pemerintahan Berbasis Elektronik, domain keamanan Sistem Pemerintahan Berbasis Elektronik, dan kebijakan internal manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik di seluruh Instansi Penyelenggara Negara | 100% | - | - | - | - | Pemerintah Pusat: Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi; Badan Siber dan Sandi Negara<br><br>Pemerintah Daerah: Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi; Kementerian Dalam Negeri; Badan Siber dan Sandi Negara | - |
| | | 3. Menyelenggarakan pembinaan dalam rangka penyelarasan kebijakan, | Terlaksananya implementasi kebijakan, penerapan standar, dan pelaksanaan | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Instansi Penyelenggara Negara |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | penerapan standar, dan pelaksanaan audit keamanan Sistem Pemerintahan Berbasis Elektronik | audit keamanan pada Sistem Pemerintahan Berbasis Elektronik | | | | | | | |
| **Fokus Area 2 : Manajemen Risiko** | | | | | | | | | | |
| 2.1. Pengoptimalan identifikasi risiko, analisis risiko, dan tindak lindung risiko Keamanan Siber | | | | | | | | | | |
| 1. Penyelenggaraan manajemen risiko Kemanan Siber yang belum maksimal dilaksanakan oleh semua sektor<br><br>2. Tingkat kesadaran implementasi manajamen risiko masih rendah<br><br>3. Pemahaman mengenai risiko siber yang belum standar dari masing-masing pemilik risiko termasuk pada level Instansi Penyelenggara Negara | Terselenggaranya manajeman risiko Keamanan Siber | 1. Menyelenggarakan sistem pengamanan dalam penyelenggaraan sistem elektronik | Penyelenggara sistem elektronik yang telah menerapkan standar keamanan yang sesuai dengan kategori sistem elektronik berbasis risiko | 20% | 40% | 60% | 80% | 100% | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 2. Menyusun profil risiko Keamanan Siber pada sektor infrastruktur informasi vital | Tersedianya profil risiko Keamanan Siber | 2 Sektor | 4 Sektor | 6 Sektor | 8 Sektor | 9 Sektor | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 3. Melakukan penilaian risiko Keamanan Siber nasional *(national risk assessment)* | Tersedianya dokumen penilaian risiko nasional | - | 1 Dokumen | - | 1 Dokumen | - | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | | | | | | | | | Presiden Nomor 82 Tahun 2022 |
| 2.2. Peningkatan efektivitas mitigasi risiko Keamanan Siber nasional | | | | | | | | | | |
| 1. *Database* penanganan risiko Keamanan Siber belum terstandar | Termanfaatkannya rekomendasi penanganan risiko Keamanan Siber nasional oleh Pemangku Kepentingan | 1. Memantau tindak lanjut rekomendasi penanganan risiko sesuai hasil penilaian risiko nasional *(national risk assessment)* | Tersedianya laporan pemantauan tindak lanjut rekomendasi penanganan risiko yang dilakukan oleh Pemangku Kepentingan sesuai hasil penilaian risiko nasional *(national risk assessment)* | - | - | 1 Dokumen | 1 Dokumen | 1 Dokumen | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 2.3. Peningkatan sinergi dan kolaborasi para Pemangku Kepentingan | | | | | | | | | | |
| 1. Budaya berbagi informasi terkait mitigasi risiko Keamanan Siber belum maksimal<br><br>2. Kolaborasi terkait mitigasi Keamanan Siber para Pemangku Kepentingan masih lemah | Meningkatnya sinergi dan kolaborasi para Pemangku Kepentingan | 1. Melakukan kolaborasi dalam penyusunan daftar *common threat vector* pada sektor | Tersedianya daftar *common threat vector* pada sektor | 1 Sektor | 3 Sektor | 5 Sektor | 7 Sektor | 8 Sektor | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 2.4. Peningkatan kualitas penyusunan dan implementasi kebijakan Keamanan Siber berbasis risiko | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Risiko terhadap Keamanan Siber semakin kompleks dan meningkat<br><br>2. Kebijakan Keamanan Siber harus diperbarui | Meningkatnya kualitas penyusunan dan implementasi kebijakan Keamanan Siber berbasis risiko | 1. Melakukan pelatihan teknis dalam penyusunan kebijakan Keamanan Siber berbasis risiko kepada Kementerian atau Lembaga dari sektor infrastruktur informasi vital | Terselenggaranya pelatihan teknis kepada Kementerian atau Lembaga dari sektor infrastruktur informasi vital terkait penyusunan kebijakan Keamanan Siber berbasis risiko | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| **Fokus Area 3 : Kesiapsiagaan dan Ketahanan** | | | | | | | | | | |
| 3.1. Pembangunan kapabilitas tanggap insiden siber yang efektif dan efisien | | | | | | | | | | |
| 1. Penanganan insiden siber belum terkoordinasi dan terkelola secara maksimal<br><br>2. Jumlah insiden siber yang terus meningkat | Terselenggaranya tanggap insiden siber yang efektif dan efisien | 1. Menyelenggarakan pembentukan tim tanggap insiden siber | Terselenggaranya asistensi pembentukan tim tanggap insiden siber | 7 Program | 7 Program | 7 Program | 7 Program | 7 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | | Terbentuknya tim tanggap insiden siber organisasi dan/atau sektor | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | | Terselenggaranya pertemuan tahunan Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*) | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 2. Menyelenggarakan peningkatan penyelenggaraan pengelolaan insiden siber | Terselenggaranya bimbingan teknis dan/atau *workshop* pengelolaan insiden siber | 7 Program | 7 Program | 7 Program | 7 Program | 7 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 3.2. Perumusan dan penetapan rencana kontingensi untuk pengelolaan krisis siber | | | | | | | | | | |
| 1. Belum adanya rencana kontingensi pengelolaan krisis siber | Tersusunnya rencana kontingensi untuk pengelolaan krisis siber | 1. Menyusun rencana kontigensi krisis siber | Tersedianya rencana kontingensi krisis siber | - | 1 Dokumen | - | - | - | Badan Siber dan Sandi Negara | Badan Nasional Penanggulangan Bencana; Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | 2. Melaksanakan simulasi rencana kontingensi krisis siber | Terselenggaranya simulasi rencana kontingensi krisis siber | - | - | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Badan Nasional Penanggulangan Bencana; Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 3.3. Penyelenggaraan penanganan tanggap darurat | | | | | | | | | | |
| 1. Penanganan tanggap darurat Keamanan Siber belum terkoordinasi dan terkelola | Terselenggaranya penanganan tanggap darurat | 1. Menyelenggarakan penanganan tanggap darurat | Tertanganinya insiden siber yang terjadi | 80% | 85% | 90% | 92% | 95% | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 3.4. Penguatan pertukaran informasi yang aman dan memiliki waktu akses yang tinggi | | | | | | | | | | |
| 1. Budaya berbagi informasi terkait tanggap darurat Keamanan Siber belum maksimal | Tersedianya informasi terkait tanggap darurat Keamanan Siber | 1. Menyelenggarakan program *Information Sharing and Analysis Center (ISAC)* | Terselenggaranya program *Information Sharing and Analysis Center (ISAC)* | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | 2. Menyelenggarakan *Voluntary Vulnerability Identification Protection (VVIP) Program* | Jumlah Pemangku Kepentingan yang berpartisipasi dalam *Voluntary Vulnerability Identification Protection (VVIP) Program* | 5 Pemangku Kepentingan | 20 Pemangku Kepentingan | 30 Pemangku Kepentingan | 35 Pemangku Kepentingan | 40 Pemangku Kepentingan | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 3. Menyelenggarakan penanganan ancaman dan serangan siber sosial | Terselenggaranya penanganan ancaman dan serangan siber sosial | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian Komunikasi dan Informatika; Kepolisian Negara Republik Indonesia; Komisi Penyiaran Indonesia; Komisi Informasi; Badan Nasional Penanggulangan Terorisme |
| **Fokus Area 4 : Penguatan Pelindungan Infrastruktur Informasi Vital** | | | | | | | | | | |
| 4.1. Penyelenggaraan pelindungan infrastruktur informasi vital | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Ancaman dan serangan siber yang sering menyasar infrastruktur informasi vital<br><br>2. Penyelenggaraan pelindungan infrastruktur informasi vital belum berjalan sepenuhnya | Terselenggaranya pelindungan infrastruktur informasi vital | 1. Melakukan identifikasi penyelenggara infrastruktur informasi vital pada setiap sektor | Tersedianya rekapitulasi hasil identifikasi penyelenggara infrastruktur informasi vital pada setiap sektor | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 2. Melakukan asistensi implementasi pelindungan infrastruktur informasi vital:<br>a. peningkatan keamanan pada sisi aplikasi, jaringan intra, pusat data, sistem penghubung layanan;<br>b. peningkatan kapasitas dan kapabilitas sumber daya manusia Keamanan Siber di seluruh sektor | Terlaksananya asistensi implementasi pelindungan infrastruktur informasi vital | - | 8 Program | 8 Program | 8 Program | 8 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | 3. Menyelenggarakan penguatan sistem operasi Keamanan Siber untuk pelindungan infrastruktur informasi vital | Jumlah Pemangku Kepentingan pada infrastruktur informasi vital yang termonitor | 12 Pemangku Kepentingan | 12 Pemangku Kepentingan | 12 Pemangku Kepentingan | 12 Pemangku Kepentingan | 12 Pemangku Kepentingan | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 4.2. Peningkatan pembinaan dan pengawasan penyelenggaraan pelindungan infrastruktur informasi vital | | | | | | | | | | |
| 1. Ancaman dan serangan siber yang sering menyasar infrastruktur informasi vital<br><br>2. Penyelenggaraan pelindungan infrastruktur informasi vital belum berjalan sepenuhnya | Meningkatnya pembinaan dan pengawasan penyelenggaraan pelindungan infrastruktur informasi vital | 1. Menyelenggarakan pengukuran tingkat kematangan Keamanan Siber di sektor infrastruktur informasi vital | Tersedianya hasil rekapitulasi pengukuran tingkat kematangan Keamanan Siber pada sektor infrastruktur informasi vital | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 2. Menyelenggarakan rapat koordinasi pelindungan infrastruktur informasi vital | Terselenggaranya forum koordinasi nasional pelindungan infrastruktur informasi vital dengan instansi pembina dan pengawas pada masing-masing sektor infrastruktur informasi vital | 1 Forum | 1 Forum | 1 Forum | 1 Forum | 1 Forum | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 3. Monitoring penyusunan dan | Tersedianya hasil monitoring | 1 Dokumen | 1 Dokumen | 1 Dokumen | 1 Dokumen | 1 Dokumen | Badan Siber dan Sandi Negara | Kementerian atau Lembaga |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| | | penetapan peta jalan pelindungan infrastruktur informasi vital | penyusunan dan penetapan peta jalan pelindungan infrastruktur informasi vital | | | | | | | dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | 4. Menyelenggarakan kajian pengembangan penyelenggaraan pelindungan infrastruktur informasi vital | Tersedianya dokumen kajian berupa strategi pengembangan penyelenggaraan pelindungan infrastruktur informasi vital nasional yang dapat digunakan oleh Pemangku Kepentingan dalam perencanaan pengembangan, pemetaan kebutuhan, dan prioritisasi kontrol keamanan pelindungan sesuai peta risiko Keamanan Siber nasional | - | - | - | 1 Dokumen | - | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| **Fokus Area 5 : Kemandirian Kriptografi Nasional** | | | | | | | | | | |
| 5.1. Penetapan kebijakan kriptografi nasional | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Kebijakan yang mengatur kriptografi belum lengkap, menyeluruh, dan detail | Tersusunnya kebijakan kriptografi nasional | 1. Menyusun kebijakan penyelenggaraan algoritma kriptografi Indonesia | Tersedianya kebijakan penyelenggaraan algoritma kriptografi Indonesia | - | 2 Dokumen | - | - | 1 Dokumen | Badan Siber dan Sandi Negara | Badan Standardisasi Nasional; Kementerian Perindustrian; Kementerian Perdagangan; Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 5.2. Peningkatan riset, pengembangan, dan inovasi di bidang kriptografi untuk mendukung pembangunan nasional | | | | | | | | | | |
| 1. Riset dan inovasi di bidang kriptografi masih terbatas<br>2. Industri kriptografi belum berkembang | Terselenggaranya riset, pengembangan, dan inovasi di bidang kriptografi untuk mendukung pembangunan nasional | 1. Menyusun rencana prioritas riset dan inovasi di bidang kriptografi dan aplikasinya | Tersedianya rencana prioritas riset dan inovasi di bidang kriptografi dan aplikasinya | - | 1 Dokumen | - | - | - | Badan Siber dan Sandi Negara, Badan Riset dan Inovasi Nasional | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 5.3. Penerapan kebijakan kriptografi nasional pada Pemangku Kepentingan | | | | | | | | | | |
| 1. Penerapan fungsi kriptografi untuk mendukung keamanan sistem | 1. Kepatuhan penerapan kebijakan kriptografi pada | 1. Melakukan evaluasi kepatuhan penerapan kebijakan kriptografi nasional | Terselenggaranya diseminasi kebijakan kriptografi nasional | - | 50 Penyeleng-gara sistem elektronik | 50 Penyeleng-gara sistem elektronik | - | - | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| elektronik belum secara masif atau terencana dengan baik oleh setiap Pemangku Kepentingan | Pemangku Kepentingan<br>2. Terselenggaranya penerapan modul kriptografi minimal pada sistem elektronik strategis atau aplikasi Sistem Pemerintahan Berbasis Elektronik prioritas nasional yang dimiliki para Pemangku Kepentingan | di sektor infrastruktur informasi vital | di sektor infrastruktur informasi vital terhadap Pemangku Kepentingan | | | | | | | Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | | Jumlah penyelenggara sistem elektronik yang menerapkan kebijakan kriptografi nasional di sektor infrastruktur informasi vital | - | - | 5 Penyeleng-gara sistem elektronik | 10 Penyeleng-gara sistem elektronik | 15 Penyeleng-gara sistem elektronik | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| | | | Data pokok Sistem Pemerintahan Berbasis Elektronik yang menerapkan kebijakan kriptografi nasional | 20% | 40% | 60% | 80% | 100% | Badan Siber dan Sandi Negara | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 |
| 5.4. Pembangunan dan pengembangan industri kriptografi nasional | | | | | | | | | | |
| 1. Industri kriptografi belum berkembang | Tumbuhnya industri kriptografi nasional | 1. Memberikan pembinaan industri kriptografi dalam negeri | Terselenggaranya asistensi dan pendampingan terhadap pelaksanaan | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian Perindustrian; Badan Riset dan Inovasi Nasional |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 2. Penerapan kriptografi masih rendah | | | industri kriptografi dalam negeri | | | | | | | |
| **Fokus Area 6 : Peningkatan Kapabilitas, Kapasitas, dan Kualitas** | | | | | | | | | | |
| 6.1. Pengembangan kurikulum berkaitan dengan Keamanan Siber pada pendidikan anak usia dini, pendidikan dasar, pendidikan menengah, dan pendidikan tinggi | | | | | | | | | | |
| 1. Tingkat pemahaman yang masih rendah dan kerentanan bagi peserta didik dalam beraktivitas di ruang siber<br><br>2. Pendidikan terkait etika di ruang siber belum diatur | Tersusunnya kurikulum Keamanan Siber | 1. Menyusun kurikulum berkaitan dengan Keamanan Siber | Tersedianya kurikulum berkaitan dengan Keamanan Siber pada pendidikan usia dini, pendidikan dasar, pendidikan menengah, dan pendidikan tinggi | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi | Badan Siber dan Sandi Negara |
| 6.2. Pengembangan dan penerapan program keterampilan dan pelatihan sumber daya manusia | | | | | | | | | | |
| 1. Masih terbatasnya Lembaga Sertifikasi Profesi bidang Keamanan Siber<br><br>2. Masih terbatasnya | Terselenggaranya program keterampilan dan pengembangan sumber daya manusia | 1. Mendorong Pembentukan Lembaga Sertifikasi Profesi Keamanan Siber/teregister Badan Siber dan Sandi Negara | Terekomendasinya/ teregisternya Lembaga Sertifikasi Profesi Keamanan Siber | 1 Lembaga Sertifikasi Profesi | 1 Lembaga Sertifikasi Profesi | 1 Lembaga Sertifikasi Profesi | 1 Lembaga Sertifikasi Profesi | 1 Lembaga Sertifikasi Profesi | Badan Siber dan Sandi Negara | Lembaga Sertifikasi Profesi/calon Lembaga Sertifikasi Profesi; Badan Nasional Sertifikasi Profesi |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| kepakaran di bidang Keamanan Siber | | 2. Melaksanakan peningkatan kapasitas sumber daya manusia pada sektor infrastruktur informasi vital | Terselenggaranya program peningkatan kapasitas sumber daya manusia pada sektor infrastruktur informasi vital | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 | Badan Siber dan Sandi Negara; Badan Nasional Sertifikasi Profesi |
| 6.3. Pengembangan dan penerapan program peningkatan kesadaran Keamanan Siber yang terkoordinasi dan berkesinambungan | | | | | | | | | | |
| 1. Tingkat kesadaran Keamanan Siber masyarakat masih rendah dan belum terkoordinasi<br><br>2. Kejahatan siber terus meningkat | Meningkatnya kesadaran Keamanan Siber masyarakat | 3. Menyelenggarakan kampanye kesadaran Keamanan Siber guna membangun budaya Keamanan Siber | Terselenggaranya program kesadaran Keamanan Siber | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Pemangku Kepentingan sesuai Peraturan Presiden Nomor 47 Tahun 2023 |
| 6.4. Penguatan kapasitas teknologi Keamanan Siber | | | | | | | | | | |
| 1. Pelaku industri teknologi Keamanan Siber masih terbatas<br><br>2. Riset dan inovasi terkait teknologi | Meningkatnya kapasitas teknologi Keamanan Siber | 1. Melakukan penumbuh-kembangan industri Keamanan Siber | Terselenggaranya program penumbuh-kembangan industri Keamanan Siber nasional | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Kementerian Perindustrian | Badan Siber dan Sandi Negara; Badan Standardisasi Nasional; Kementerian Perdagangan |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Keamanan Siber masih rendah<br><br>3. Penerapan *common criteria* teknologi Keamanan Siber masih terbatas | | | | | | | | | | |
| 6.5. Peningkatan riset, pengembangan, dan inovasi ilmu pengetahuan dan teknologi di bidang Keamanan Siber | | | | | | | | | | |
| 1. Riset dan inovasi terkait teknologi Keamanan Siber masih rendah | Meningkatnya riset, pengembangan, dan inovasi ilmu pengetahuan teknologi di bidang Keamanan Siber | 1. Mendorong kemitraan dan kolaborasi riset Pemangku Kepentingan yang tepat guna | Terlaksananya riset bersama antara pemerintah, akademisi, pelaku usaha, dan komunitas di bidang kriptografi dan aplikasinya | - | - | - | 1 Kegiatan | - | Badan Riset dan Inovasi Nasional | Badan Siber dan Sandi Negara; Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi; Kementerian Komunikasi dan Informatika; Kementerian Perdagangan |
| | | 2. Menyusun peta jalan penelitian Keamanan Siber | Tersedianya peta jalan penelitian Keamanan Siber | - | - | 1 Dokumen | - | - | Badan Riset dan Inovasi Nasional | Badan Siber dan Sandi Negara |
| 6.6. Pengembangan program yang khusus untuk sektor dan kelompok rentan sesuai dengan kebutuhan | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Program Pendidikan untuk kelompok rentan belum mengatur tentang Keamanan Siber<br><br>2. Ancaman dan kejahatan siber menarget kepada kelompok rentan | Terselenggaranya program khusus bagi sektor dan kelompok rentan | 1. Melaksanakan program pelindungan anak dan perempuan di ruang siber termasuk pemberdayaan perempuan di ruang siber | Terselenggaranya program pelindungan anak dan perempuan di ruang siber | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Kementerian Pemberdayaan Perempuan dan Perlindungan Anak | Badan Siber dan Sandi Negara; Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi; Kementerian Komunikasi dan Informatika |
| | | 2. Melaksanakan program pelindungan kelompok lanjut usia di ruang siber | Terselenggaranya program pelindungan kelompok lanjut usia di ruang siber | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian Sosial |
| | | 3. Melaksanakan program pelindungan kelompok difabel di ruang siber | Terselenggaranya program pelindungan kelompok difabel di ruang siber | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian Sosial |
| **Fokus Area 7 : Kebijakan Keamanan Siber** | | | | | | | | | | |
| 7.1. Analisis dan evaluasi terhadap kebijakan Keamanan Siber | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Adanya kebijakan penerapan indeks kualitas kebijakan | Tersusunnya analisis dan evaluasi kebijakan Keamanan Siber | 1. Melakukan analisis dan evaluasi peraturan perundang-undangan terkait dengan Keamanan Siber | Laporan analisis dan evaluasi atau rekomendasi terkait dengan peraturan perundang-undangan bidang Keamanan Siber dan sandi | 1 Kegiatan | 1 Kegiatan | 1 Kegiatan | 1 Kegiatan | 1 Kegiatan | Badan Siber dan Sandi Negara | Kementerian Hukum dan Hak Asasi Manusia |
| 7.2. Perumusan dan pemberian rekomendasi kebijakan di bidang Keamanan Siber | | | | | | | | | | |
| 1. Amanat peraturan pelaksanaan pada peraturan perundang-undangan terkait Keamanan Siber | Tersusunnya rekomendasi kebijakan Keamanan Siber | 1. Menyusun kebijakan /peraturan pelaksanaan bidang Keamanan Siber dan Sandi | Tingkat penyelesaian kebijakan/peraturan pelaksana dalam Peraturan Presiden atau Peraturan Pemerintah di bidang Keamanan Siber dan sandi | 100% | 100% | 100% | 100% | 100% | Badan Siber dan Sandi Negara | Kementerian Hukum dan Hak Asasi Manusia |
| | | 2. Menyusun peta jalan pelindungan infrastruktur informasi vital pada semua sektor infrastruktur informasi vital | Tersusunnya peta jalan pelindungan infrastruktur informasi vital pada semua sektor infrastruktur informasi vital | 1 Sektor | 3 Sektor | - | - | - | Kementerian atau Lembaga dari sektor Infrastruktur Informasi Vital sesuai Peraturan Presiden Nomor 82 Tahun 2022 | Badan Siber dan Sandi Negara |
| 7.3. Pembudayaan hukum dan peningkatan kesadaran hukum masyarakat | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Tingkat kesadaran hukum masyarakat terkait Keamanan Siber masih rendah | Terbentuknya budaya hukum dan kesadaran hukum masyarakat | 1. Melakukan penyuluhan hukum langsung dan tidak langsung | Meningkatnya pengetahuan dan pemahaman hukum masyarakat terhadap peraturan perundang-undangan | 1 Kegiatan | 1 Kegiatan | 1 Kegiatan | 1 Kegiatan | 1 Kegiatan | Badan Siber dan Sandi Negara | Kementerian Hukum dan Hak Asasi Manusia |
| 7.4. Penegakan hukum di bidang Keamanan Siber secara terpadu | | | | | | | | | | |
| 1. Ancaman siber semakin meningkat<br>2. Penegakan hukum terkait Keamanan Siber belum maksimal | Terbentuknya penegakan hukum di bidang Keamanan Siber secara terpadu | 1. Menyelenggarakan forum koordinasi penegakan hukum dalam menangani insiden siber | Terbentuknya forum koordinasi penegak hukum dalam menangani insiden siber | - | 1 Forum | - | - | - | Kepolisian Negara Republik Indonesia | Badan Siber dan Sandi Negara; Kejaksaan Republik Indonesia; Kementerian Komunikasi dan Informatika; Badan Nasional Penanggulangan Terorisme |
| | | 2. Menyediakan sarana pengaduan hukum di bidang kejahatan siber untuk masyarakat | Tersedianya program pelayanan pengaduan hukum terpadu yang aman dan akuntabel | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Kepolisian Negara Republik Indonesia | Badan Siber dan Sandi Negara; Kejaksaan Republik Indonesia; Kementerian Komunikasi dan Informatika |
| **Fokus Area 8 : Kerja Sama internasional** | | | | | | | | | | |
| 8.1. Penetapan kebijakan dan prioritas kerja sama internasional di bidang Keamanan Siber | | | | | | | | | | |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1. Belum adanya kebijakan dan *roadmap* terkait kerja sama internasional di bidang Keamanan Siber<br><br>2. Inisiasi dari negara asing terkait kerja sama bidang Keamanan Siber semakin meningkat | Tersusunnya kebijakan dan prioritas kerja sama internasional Keamanan Siber | 1. Mendukung kebijakan politik luar negeri bebas aktif di bidang Keamanan Siber | Rekomendasi kebijakan terkait Keamanan Siber yang diadopsi dalam forum internasional | - | - | - | 1 Dokumen | - | Badan Siber dan Sandi Negara | Instansi Penyelenggara Negara |
| | | | Pedoman kerja sama internasional di bidang Keamanan Siber | - | - | 1 Dokumen | - | - | Badan Siber dan Sandi Negara | Kementerian Luar Negeri |
| 8.2. Peningkatan inisiatif kerja sama internasional dalam rangka mendukung terciptanya ruang siber yang aman, damai, dan terbuka serta meningkatkan kapasitas nasional di bidang Keamanan Siber | | | | | | | | | | |
| 1. Inisiasi dari negara asing terkait kerja sama bidang Keamanan Siber semakin meningkat | Meningkatnya reputasi Indonesia secara internasional dalam bidang Keamanan Siber | 1. Menginisiasi program *confidence building measures* bidang Keamanan Siber dengan negara lain | Jumlah program *confidence building measures* bidang Keamanan Siber dengan negara mitra | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian Luar Negeri; Badan Nasional Penanggulangan Terorisme; Kepolisian Negara Republik Indonesia |
| 8.3. Peningkatan kerja sama praktis, berbagi informasi, dan praktek terbaik dalam menghadapi krisis siber | | | | | | | | | | |
| 1. Forum berbagi informasi antarnegara dalam menghadapi krisis siber masih rendah<br>2. Pengalaman dan pembelajaran | Terselenggaranya kerja sama dalam menghadapi krisis siber | 1. Melaksanakan program kerja sama antara *National Computer Security Incident Response Team* dengan negara lain dan/atau dengan organisasi internasional dalam | Terselenggaranya program kerja sama antara *National Computer Security Incident Response Team* dengan negara lain dan/atau dengan organisasi | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Badan Siber dan Sandi Negara | Kementerian Luar Negeri |

| Tantangan | Sasaran Strategis | Kegiatan | Indikator Keberhasilan | Target dan Tahun Capaian | | | | | Penanggung Jawab | Instansi Terkait |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 2024 | 2025 | 2026 | 2027 | 2028 | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| dalam menghadapi krisis siber di dalam negeri masih rendah | | rangka menghadapi krisis siber | internasional dalam rangka menghadapi krisis siber | | | | | | | |
| 8.4. Peningkatan peran Indonesia dalam forum bilateral, regional, dan multilateral di bidang Keamanan Siber | | | | | | | | | | |
| 1. Kontribusi Indonesia dalam forum internasional bidang Keamanan Siber perlu ditingkatkan<br><br>2. Forum internasional terkait Keamanan Siber semakin meningkat | Meningkatnya peran Indonesia dalam forum internasional di bidang Keamanan Siber | 1. Meningkatkan peran negara dalam forum internasional | Terselenggaranya program yang dapat ditindaklanjuti dari kegiatan forum internasional | 1 Program | 1 Program | 1 Program | 1 Program | 1 Program | Kementerian Luar Negeri | Badan Siber dan Sandi Negara |
| | | 2. Melakukan kerja sama bilateral di bidang Keamanan Siber | Jumlah perjanjian kerja sama bilateral di bidang Keamanan Siber | 3 Negara | 1 Negara | 2 Negara | 1 Negara | 3 Negara | Badan Siber dan Sandi Negara | Kementerian Luar Negeri |

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN