



KEMENTERIAN KOORDINATOR BIDANG HUKUM,
HAK ASASI MANUSIA, IMIGRASI, DAN PEMASYARAKATAN
REPUBLIK INDONESIA

KEPUTUSAN SEKRETARIS KEMENTERIAN KOORDINATOR BIDANG
HUKUM, HAK ASASI MANUSIA, IMIGRASI, DAN PEMASYARAKATAN
NOMOR SES-TI.03.02-269 TAHUN 2025

TENTANG

PENETAPAN

TIM TANGGAP INSIDEN SIBER

KEMENTERIAN KOORDINATOR BIDANG HUKUM, HAK ASASI
MANUSIA, IMIGRASI, DAN PEMASYARAKATAN

SEKRETARIS KEMENTERIAN KOORDINATOR BIDANG HUKUM,
HAK ASASI MANUSIA, IMIGRASI, DAN PEMASYARAKATAN,

Menimbang : a. bahwa pemanfaatan teknologi informasi dan komunikasi maupun teknologi terkait dapat menyebabkan kerawanan dan ancaman siber yang meliputi aspek kerahasiaan, keutuhan, ketersediaan, nir-sangkal, otentisitas, akuntabilitas dan keandalan layanan, sehingga dibutuhkan penyediaan pelayanan publik yang cepat, andal, dan aman;

b. bahwa penyelenggara sistem elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan, penanggulangan dan pemulihan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian;

c. bahwa untuk menjamin sistem elektronik dapat beroperasi secara terus menerus, maka diperlukan mekanisme penanggulangan insiden dan/atau pemulihan insiden yang dilakukan oleh tim penanggulangan dan pemulihan insiden siber;

d. bahwa untuk melaksanakan kegiatan sebagaimana dimaksud dalam huruf c, diperlukan Pembentukan Tim Tanggap Insiden Siber Kementerian Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi dan Pemasyarakatan RI-*Computer Security Incident Response Team* (KEMENKO KUMHAMIMPAS-CSIRT);

e. bahwa untuk memenuhi ketentuan sebagaimana dimaksud pada huruf a, b, c dan d, dipandang perlu menetapkan Keputusan Sekretaris Kementerian Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi, dan Pemasyarakatan tentang Penetapan Tim Tanggap Insiden Siber Kementerian Koordinator Bidang Hukum,

Hak Asasi Manusia, Imigrasi dan Pemasyarakatan RI (KEMENKO KUMHAMIMIPAS-CSIRT).

- Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 15 dan 16 (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
2. Peraturan Presiden No.95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) Pasal 40 dan 41 (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182); dan
3. Peraturan Badan Siber dan Sandi Negara No 1 Tahun 2024 tentang Pengelolaan Insiden Siber.

MEMUTUSKAN :

- Menetapkan : KEPUTUSAN SEKRETARIS KEMENTERIAN KOORDINATOR BIDANG HUKUM, HAK ASASI MANUSIA, IMIGRASI, DAN PEMASYARAKATAN TENTANG PENETAPAN TIM TANGGAP INSIDEN SIBER KEMENTERIAN KOORDINATOR BIDANG HUKUM, HAK ASASI MANUSIA, IMIGRASI, DAN PEMASYARAKATAN DENGAN NAMA KEMENKO KUMHAMIMIPAS-CSIRT.
- KESATU : Membentuk Tim Tanggap Insiden Siber Kementerian Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi, dan Pemasyarakatan (KEMENKO KUMHAMIMIPAS-CSIRT) dengan susunan sebagaimana tercantum dalam lampiran yang merupakan bagian yang tidak terpisahkan dari keputusan ini.
- KEDUA : KEMENKO KUMHAMIMIPAS-CSIRT mempunyai layanan, berupa :
1. Penanggulangan dan Pemulihan Insiden Siber, yaitu :
a. Deteksi Insiden;
b. Analisis Insiden;
c. Penilaian Risiko Keamanan Siber dan Mitigasi Insiden Siber; dan
d. Pemulihan.
2. Penyampaian Informasi Insiden Siber Kepada Pihak Terkait.
3. Diseminasi Informasi untuk Mencegah dan/atau Mengurangi Dampak dari Insiden Siber.
- KETIGA : Dalam melaksanakan layanan tersebut, TTIS memiliki fungsi utama dan fungsi lainnya sesuai kebutuhan, yaitu :
1. Pemberian peringatan terkait Keamanan Siber;

2. Perumusan panduan teknis penanganan Insiden Siber;
3. Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
4. Pemilahan (*triage*) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;
5. Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan
6. Diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

KEEMPAT : KEMENKO KUMHAMIMIPAS-CSIRT memiliki konstituen yaitu pengguna Teknologi Informasi dan Komunikasi (TIK) di lingkungan KEMENKO KUMHAMIMIPAS-CSIRT.

KELIMA : KEMENKO KUMHAMIMIPAS-CSIRT mempunyai susunan tim dengan tugas dan tanggung jawab sebagai berikut :

1. Ketua, mempunyai tugas dan tanggung jawab yaitu :
 - a. Memimpin pelaksanaan tugas dan bertanggung jawab atas kegiatan di KEMENKO KUMHAMIMIPAS-CSIRT;
 - b. Menyediakan *Point of Contact* (POC) untuk KEMENKO KUMHAMIMIPAS-CSIRT, berupa alamat email, nomor telepon, dan komunikasi lainnya;
 - c. Bertanggung jawab dalam pengalokasian sumber daya yang dibutuhkan untuk mengoperasionalkan layanan KEMENKO KUMHAMIMIPAS-CSIRT;
 - d. Mengkoordinasikan KEMENKO KUMHAMIMIPAS-CSIRT dengan instansi dan pihak-pihak terkait lainnya dalam rangka pelaksanaan tugas dan fungsi KEMENKO KUMHAMIMIPAS-CSIRT, serta menjalin kerja sama antar CSIRT;
 - e. Memantau operasional dan kinerja KEMENKO KUMHAMIMIPAS-CSIRT;
 - f. Membuat perencanaan operasional dan strategis mengenai KEMENKO KUMHAMIMIPAS-CSIRT;
 - g. Mengkoordinasikan edukasi dan pelatihan mengenai keamanan siber di lingkungan KEMENKO KUMHAMIMIPAS-CSIRT; dan
 - h. Menyusun dan menyampaikan laporan kepada Menteri Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi, dan Pemasyarakatan.
2. Sekretaris, mempunyai tugas dan tanggung jawab yaitu:
 - a. Melaksanakan fungsi kesekretariatan/ketatausahaan meliputi administrasi dan

dokumentasi pada operasional layanan KEMENKO KUMHAMIMIPAS-CSIRT;

- b. Menyusun, memelihara, dan mengevaluasi dokumen kebijakan, standar, dan prosedur keamanan informasi pada organisasi TTIS;
- c. Menyusun metrik pengukuran tingkat kematangan penerapan keamanan informasi pada organisasi TTIS; dan
- d. Menyusun metrik pengukuran evaluasi tingkat kematangan dan kinerja organisasi TTIS.

3. Unit Monitoring dan Aksi:

Unit ini dipimpin oleh seorang Ketua Unit dan mempunyai tugas dan tanggung jawab yaitu :

- a. Melakukan pemantauan terhadap jaringan, sistem, dan aplikasi untuk mendeteksi aktivitas yang mencurigakan atau anomali;
- b. Menggunakan alat pemantauan jaringan dan sistem seperti SIEM (*Security Information and Event Management*), IDS/IPS (*Intrusion Detection/Prevention Systems*), dan alat pemantauan log;
- c. Menganalisis log sistem dan peristiwa keamanan untuk mengidentifikasi tanda-tanda kompromi atau serangan;
- d. Mengidentifikasi pola dan indikator ancaman (*Indicators of Compromise - IoCs*) yang dapat menunjukkan adanya aktivitas berbahaya;
- e. Melakukan monitoring pendekripsi serangan;
- f. Menyampaikan pemberian peringatan terkait keamanan siber kepada para pihak terkait;
- g. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan monitoring;
- h. Membuat, memelihara dan mengevaluasi standar operasional dan prosedur proses tanggap Insiden Siber;
- i. Memberikan asistensi dan/atau bantuan terkait tanggap Insiden Siber kepada konstituen TTIS;
- j. Melakukan pemilahan (*triage*) Insiden Siber sesuai kriteria yang ditetapkan;
- k. Melakukan penanganan artefak digital;
- l. Melakukan akuisisi dan preservasi data dan informasi yang diperlukan dalam proses investigasi atau tanggap Insiden Siber;
- m. Membuat laporan proses tanggap Insiden Siber yang dilakukan;

- n. Melakukan pengelolaan, pendokumentasian terhadap laporan tanggap Insiden Siber;
- o. Membuat publikasi terkait dengan *best practices proses* tanggap Insiden Siber;
- p. Melakukan analisis terhadap Insiden Siber yang terjadi yang diperoleh dari hasil kerjasama ataupun dari *news feed* yang ada di media sosial untuk menjadi *lesson learned* kepada konstituen TTIS dan forum berbagi koordinasi dan komunikasi TTIS;
- q. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan tanggap insiden;
- r. Melakukan pemindaian kerentanan secara berkala terhadap aset konstituen TTIS;
- s. Mengidentifikasi kerentanan dalam sistem;
- t. Menilai dampak potensial dari kerentanan;
- u. Melakukan penanganan kerentanan sistem elektronik;
- v. Menyusun laporan kerentanan secara berkala berdasarkan konstituen TTIS; dan
- w. Melakukan reviu terhadap laporan kerentanan.

4. Unit Penanganan Kerentanan:

Unit ini dipimpin oleh seorang Ketua Unit dan mempunyai tugas dan tanggung jawab yaitu :

- a. Melakukan pemantauan terhadap jaringan, sistem, dan aplikasi untuk mendeteksi aktivitas yang mencurigakan atau anomali;
- b. Mengidentifikasi kerentanan yang dieksplorasi dan laporan kerentanan sebagai bagian dari insiden keamanan;
- c. Mempelajari kerentanan baru dengan membaca sumber publik atau sumber pihak ketiga lainnya;
- d. Menemukan atau mencari kerentanan baru sebagai akibat dari aktivitas atau penelitian yang disengaja;
- e. Melakukan analisis tren dari *feed* dan data kerentanan dikumpulkan, untuk memahami konstituen atau TTP aktor serangan;
- f. Membuat perencanaan, pengelolaan dan evaluasi kegiatan pada bagian teknis penelitian dan pelaporan kerentanan.
- g. Melakukan pemindaian kerentanan secara berkala terhadap aset konstituen TTIS;

- h. Melakukan pengumpulan, pengolahan, dan analisis kerentanan keamanan siber lainnya yang mencakup ancaman, kerentanan, dan produk/perangkat TI;
- i. Menyusun rekomendasi dan laporan kerentanan secara berkala;
- j. Melakukan reviu terhadap laporan kerentanan;
- k. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan analisis kerentanan;
- l. Melakukan pemindaian kerentanan secara berkala terhadap aset konstituen TTIS;
- m. Memastikan pemberitahuan informasi kerentanan tepat waktu dan terdistribusi yang akurat;
- n. Menjaga arus informasi dan melacak status aktivitas entitas yang ditugaskan atau diminta untuk berpartisipasi dalam merespons insiden keamanan informasi;
- o. Memastikan rekomendasi kerentanan dilaksanakan oleh konstituen TTIS;
- p. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan koordinasi dan pengungkapan kerentanan.
- q. Memperbaiki atau memitigasi kerentanan yang ditemukan baik dari sistem monitoring dan pelaporan kerentanan untuk mencegah eksploitasi;
- r. Menerapkan *patch* atau solusi keamanan lain berdasarkan rencana tanggap insiden kerentanan dan *best practice*;
- s. Menyusun dan mendokumentasikan laporan respons kerentanan; dan
- t. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan respons kerentanan.

5. Unit Pembinaan dan Publikasi :

Unit ini dipimpin oleh seorang Ketua Unit dan mempunyai tugas dan tanggung jawab yaitu :

- a. Mengelola akun media sosial terkait dengan publikasi TTIS;
- b. Membuat strategi komunikasi untuk membangun berbagi informasi keamanan siber;
- c. Mengelola portal publikasi terkait dengan publikasi TTIS;

- d. Memperhitungkan audiens saat informasi dibuat dan disebarluaskan;
- e. Menerima masukan, laporan, komentar, dan pertanyaan dari konstituen TTIS;
- f. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan berbagi informasi;
- g. Membuat dan melaksanakan program edukasi keamanan siber;
- h. Membuat laporan publikasi mengenai kondisi terkini keamanan siber organisasi (laporan bulanan, laporan 3 bulanan, laporan 6 bulanan, dan laporan tahunan);
- i. Membuat publikasi teknis mengenai keamanan siber;
- j. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan peningkatan kesadaran keamanan siber;
- k. Membuat dan melaksanakan program pelatihan keamanan siber;
- l. Memberikan pelatihan dan pendidikan keamanan siber kepada konstituen TTIS (yang mungkin mencakup staf organisasi dan TTIS);
- m. Menilai, mengidentifikasi, dan mendokumentasikan kebutuhan kompetensi SDM untuk mengembangkan materi pelatihan dan pendidikan yang sesuai dan meningkatkan tingkat keterampilannya; dan
- n. Melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan pelatihan keamanan siber.

- KEENAM** : Dalam melaksanakan tugas, Ketua KEMENKO KUMHAMIMIPAS-CSIRT bertanggung jawab kepada Menteri Kementerian Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi, dan Pemasyarakatan.
- KETUJUH** : Untuk kelancaran pelaksanaan tugas KEMENKO KUMHAMIMIPAS-CSIRT dapat berkoordinasi dan bekerja sama dengan pihak-pihak lain.
- KEDELAPAN** : Membebankan biaya pelaksanaan tugas KEMENKO KUMHAMIMIPAS-CSIRT ini kepada Anggaran Biro Hubungan Masyarakat dan Teknologi Informasi Kementerian Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi, dan Pemasyarakatan Republik Indonesia.

KESEMBILAN : Keputusan ini berlaku sejak tanggal ditetapkan, dengan catatan bahwa apabila dikemudian hari terdapat kekeliruan dalam keputusan ini akan diadakan perubahan sebagaimana mestinya.

Ditetapkan di Jakarta
pada tanggal 01 Oktober 2025

SEKRETARIS KEMENTERIAN
KOORDINATOR BIDANG HUKUM, HAK
ASASI MANUSIA, IMIGRASI, DAN
PEMASTAKATAN RI,



R. ANDIKA DWI PRASETYA

Lampiran I
Keputusan Sekretaris Kementerian
Koordinator
Nomor : SES-TI.03.02-269 Tahun 2025
Tanggal 01 Oktober 2025

SUSUNAN TIM TANGGAP INSIDEN SIBER KEMENTERIAN KOORDINATOR
BIDANG HUKUM, HAK ASASI MANUSIA, IMIGRASI, DAN
PEMASYARAKATAN
(KEMENKO KUMHAMIMIPAS-CSIRT)

NO.	JABATAN DALAM TIM	JABATAN/NAMA PERSONIL
1.	Ketua TTIS	Kepala Biro Hubungan Masyarakat dan Teknologi Informasi Kementerian Koordinator Bidang Hukum, Hak Asasi Manusia, Imigrasi, dan Pemasyarakatan RI
2.	Sekretaris	Wisnu Firmansyah
3.	Ketua Unit Monitoring dan Aksi	Muhammad Togar Arif
	Anggota	1. Ayep Saepuloh 2. Fransisca Puspitaning Ari 3. M. Irfan Fitriadi 4. Julius Axl Adindrawi Sebastian
4.	Ketua Unit Penanganan Kerentanan	Ega Wandanu
	Anggota	1. Adrie Aryasa 2. Dwinda Harditya 3. Fristisa Indah Pratiwi 4. Rafli Aditya Priyatna
5.	Ketua Unit Pembinaan dan Publikasi	Mutia Adia Risjad
	Anggota	1. Moch. Rey Baskara 2. Andi Irsal 3. Hesnaningtyas Putria 4. Muh. Khomsin Nurul Hidayah 5. Octa Vidya Rachma 6. Khandita Wijaya 7. Muhammad Wardani

Ditetapkan di Jakarta
pada tanggal 01 Oktober 2025

SEKRETARIS KEMENTERIAN
KOORDINATOR BIDANG HUKUM,
HAK ASASI MANUSIA, IMIGRASI, DAN
PEMASYARAKATAN RI,



R. ANDIKA DWI PRASETYA

Lampiran II
Keputusan Sekretaris Kementerian
Koordinator
Nomor : SES-TI.03.02-269 Tahun 2025
Tanggal 01 Oktober 2025

BAGAN STRUKTUR ORGANISASI
TIM TANGGAP INSIDEN SIBER
KEMENTERIAN KOORDINATOR BIDANG HUKUM, HAK ASASI MANUSIA,
IMIGRASI, DAN PEMASYARAKATAN RI
(KEMENKO KUMHAMIMIPAS-CSIRT)

