SEKRETARIAT DAERAH PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA

KEPUTUSAN SEKRETARIS DAERAH PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA

NOMOR 143 TAHUN 2025

TENTANG

TIM TANGGAP INSIDEN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

SEKRETARIS DAERAH PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 21 ayat (2) Peraturan Gubernur Nomor 15 Tahun 2025 tentang Pelaksanaan Persandian untuk Pengamanan Informasi, perlu menetapkan Keputusan Sekretaris Daerah tentang Tim Tanggap Insiden Siber;

Mengingat :

1. Undang-Undang Nomor 29 Tahun 2007 tentang Pemerintahan Provinsi Daerah Khusus Ibukota Jakarta Sebagai Ibukota Negara Kesatuan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 93, Tambahan Lembaran Negara Republik Indonesia Nomor 4744);
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Peraturan Gubernur Nomor 15 Tahun 2025 tentang Pelaksanaan Persandian untuk Pengamanan Informasi (Berita Daerah Provinsi Daerah Khusus Ibukota Jakarta Tahun 2025 Nomor 71004);

MEMUTUSKAN:

Menetapkan : KEPUTUSAN SEKRETARIS DAERAH TENTANG TIM TANGGAP INSIDEN SIBER.

KESATU : Membentuk Tim Tanggap Insiden Siber dengan susunan, tugas dan tanggung jawab sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan Sekretaris Daerah ini.

KEDUA : Tim Tanggap Insiden Siber sebagaimana tercantum dalam diktum KESATU memiliki fungsi utama berupa:

1. pemberian peringatan terkait keamanan siber;
2. perumusan panduan teknis penanganan insiden siber;
3. penerimaan pencatatan setiap laporan/aduan yang dilaporkan dan 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.

KETIGA : Biaya yang diperlukan untuk pelaksanaan Keputusan Sekretaris Daerah ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah Provinsi DKI Jakarta melalui Dokumen Pelaksanaan Anggaran pada masing-masing Perangkat Daerah.

KEEMPAT : Pada saat Keputusan Sekretaris Daerah ini mulai berlaku, Keputusan Sekretaris Daerah Nomor 41 Tahun 2020 tentang *Computer Security Incident Response Team*, dicabut dan dinyatakan tidak berlaku.

KELIMA : Keputusan Sekretaris Daerah ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 22 September 2025

SEKRETARIS DAERAH PROVINSI DAERAH KHUSUS
IBUKOTA JAKARTA,

MARULLAH MATALI
NIP 196511271996031003

Tembusan:
1. Gubernur Daerah Khusus Ibukota Jakarta
2. Wakil Gubernur Daerah Khusus Ibukota Jakarta
3. Para Asisten Sekretaris Daerah Provinsi DKI Jakarta

LAMPIRAN
KEPUTUSAN SEKRETARIS DAERAH PROVINSI DAERAH KHUSUS IBUKOTA JAKARTA

NOMOR 143 TAHUN 2025

TENTANG
TIM TANGGAP INSIDEN SIBER

SUSUNAN KEANGGOTAAN, TUGAS DAN TANGGUNG JAWAB TIM TANGGAP INSIDEN SIBER

A. Susunan Tim Tanggap Insiden Siber

1. Pengarah : Sekretaris Daerah Provinsi DKI Jakarta
2. Penanggung Jawab : Asisten Pemerintahan Sekda Provinsi DKI Jakarta
3. Ketua : Kepala Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta
4. Sekretaris : Sekretaris Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta
5. Unit Pemantauan dan Aksi

   Penanggung Jawab : Kepala Bidang Siber, Sandi dan Aplikasi

   a. Fungsi Pemantauan dan Tanggap Insiden

      Koordinator : Ketua Subkelompok Pengelolaan Layanan Siber, Sandi dan Aplikasi

      Anggota :
      1) Unsur pada Subkelompok Pengelolaan Layanan Siber, Sandi dan Aplikasi
      2) Unsur pada Subkelompok Pengembangan Siber, Sandi dan Aplikasi
      3) Unsur pada Bidang Infrastruktur Digital
      4) Unsur pada Bidang Data dan Statistik
      5) Unsur pada Unit Pengelola Perangkat dan Jaringan Sistem Elektronik
      6) Unsur pada Unit Pengelola Layanan Teknologi Informasi dan Komunikasi
      7) Unsur pada Seksi Aplikasi, Siber dan Statisitik pada Suku Dinas Komunikasi, Informatika, dan Statistik Kota Administrasi

			8) Unsur pada Seksi Infrastruktur Digital pada Suku Dinas Komunikasi, Informatika, dan Statistik Kota Administrasi
			9) Unsur pada Seksi Infrastruktur Digital, Aplikasi, Siber dan Statistik pada Suku Dinas Komunikasi, Informatika, dan Statistik Kabupaten Administrasi
b. Fungsi Pengujian dan Analisis Kerentanan	Koordinator	:	Ketua Subkelompok Pemberdayaan dan Pengendalian Siber, Sandi dan Aplikasi
	Anggota	:	Unsur pada Subkelompok Pemberdayaan dan Pengendalian Siber, Sandi dan Aplikasi
6. Unit Tata Kelola	Penanggung Jawab	:	Kepala Bidang Tata Kelola Sistem Elektronik dan Transformasi Digital
	Koordinator	:	Ketua Subkelompok Tata Kelola Keamanan dan Infrastruktur
	Anggota	:	Unsur pada Subkelompok Tata Kelola Keamanan dan Infrastruktur
7. Unit Komunikasi dan Informasi	Penanggung Jawab 1	:	Kepala Bidang Komunikasi Publik
	Penanggung Jawab 2	:	Kepala Bidang Informasi Publik
	Koordinator 1	:	Ketua Subkelompok Sumber Daya Komunikasi Publik
	Koordinator 2	:	Ketua Subkelompok Pelayanan Informasi Publik
	Anggota	:	1) Unsur pada Subkelompok Sumber Daya Komunikasi Publik
			2) Unsur pada Subkelompok Pelayanan Informasi Publik
8. Agen Penanganan Insiden Siber	: Pengelola Teknologi Informasi pada Perangkat Daerah		

B. Tugas dan Tanggung Jawab

1. Pengarah : memberikan arahan, pertimbangan, dan masukan atas penyelenggaraan Tim Tanggap Insiden Siber.

2. Penanggung Jawab :
   1) menjamin terselenggaranya pengelolaan penanggulangan dan pemulihan insiden siber yang meliputi organisasi, sumber daya manusia, dan angga ran yang memadai; dan
   2) memberikan pembinaan, kebijakan, sasaran, dan petunjuk teknis dalam penyelenggaraan pengelolaan pengaduan pelayanan insiden siber.

3. Ketua :
   1) memimpin pelaksanaan tugas Tim Tanggap Insiden Siber dalam melakukan pembinaan, pengendalian, pengelolaan, dan pengawasan evaluasi terhadap operasi dan kendali serta personel; dan
   2) bertanggung jawab atas pelaksanaan operasional Tim Tanggap Insiden Siber.

4. Sekretaris :
   1) melakukan fasilitasi pelaksanaan tugas ketua Tim Tanggap Insiden Siber dalam melakukan pembinaan, pengendalian, pengelolaan, dan pengawasan evaluasi terhadap operasi dan kendali serta personel;
   2) melakukan penataan administrasi yang efisien, perencanaan organisasi, dan pengelolaan dokumentasi organisasi Tim Tanggap Insiden Siber; dan
   3) melaksanakan evaluasi rutin terhadap pelaksanaan program dan kegiatan Tim Tanggap Insiden Siber.

5. Unit Pemantauan dan Aksi

   a. Fungsi Pemantauan dan Tanggap Insiden :
      1) menerima laporan/pengaduan insiden siber;
      2) melakukan pemantauan terhadap jaringan, sistem, dan aplikasi untuk mendeteksi aktivitas yang mencurigakan atau anomali;
      3) menggunakan alat pemantauan jaringan dan sistem serta melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan *monitoring* keamanan siber;
      4) mengidentifikasi pola dan indikator ancaman (*Indicators of Compromise* - IoCs) yang dapat menunjukkan adanya aktivitas berbahaya;
      5) melakukan *monitoring* pendeteksian serangan;

6) menyampaikan pemberian peringatan terkait keamanan siber kepada para pihak terkait;

7) memberikan asistensi dan/atau bantuan terkait tanggap insiden siber kepada konstituen Tim Tanggap Insiden Siber;

8) melakukan pemilahan (*triage*) insiden siber sesuai kriteria yang ditetapkan;

9) membuat laporan proses tanggap insiden siber yang dilakukan;

10) melakukan pengelolaan, pendokumentasian terhadap laporan tanggap insiden siber;

11) membuat publikasi terkait dengan *best practices* proses tanggap insiden siber pada *website* CSIRT;

12) melakukan pengelolaan *website* CSIRT yang digunakan dalam kegiatan tanggap insiden;

13) melakukan pengelolaan *website* CSIRT yang digunakan dalam kegiatan peningkatan kesadaran keamanan siber; dan

14) melaksanakan pengukuran evaluasi tingkat kematangan dan kinerja organisasi Tim Tanggap Insiden Siber.

b. Fungsi Pengujian dan Analisis Kerentanan : 1) menganalisis log sistem dan peristiwa keamanan untuk mengidentifikasi tanda-tanda kompromi atau serangan;

2) melakukan pemindaian kerentanan secara berkala terhadap aset konstituen Tim Tanggap Insiden Siber;

3) mengidentifikasi kerentanan dalam sistem;

4) menilai dampak potensial dari kerentanan;

5) menyusun laporan kerentanan secara berkala berdasarkan konstituen Tim Tanggap Insiden Siber;

6) melakukan reviu terhadap laporan kerentanan;

7) melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan uji penetrasi;

8) mengidentifikasi kerentanan yang dieksploitasi dan laporan kerentanan sebagai bagian dari insiden keamanan;

9) mempelajari kerentanan baru dengan membaca sumber publik atau sumber pihak ketiga lainnya;

10) menemukan atau mencari kerentanan baru sebagai akibat dari aktivitas atau penelitian yang disengaja;

11) melakukan analisis tren dari *feed* dan data kerentanan dikumpulkan, untuk memahami konstituen atau Taktik, Teknik dan Prosedur (TTP) aktor serangan;

12) melakukan pemindaian kerentanan secara berkala terhadap aset konstituen Tim Tanggap Insiden Siber;

13) melakukan pengumpulan, pengolahan, dan analisis kerentanan keamanan siber lainnya yang mencakup ancaman, kerentanan, dan produk/perangkat teknologi informasi;

14) menyusun rekomendasi dan laporan kerentanan secara berkala;

15) melakukan reviu terhadap laporan kerentanan;

16) melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan analisis kerentanan;

17) memastikan pemberitahuan informasi kerentanan tepat waktu dan terdistribusi yang akurat;

18) memastikan rekomendasi kerentanan dilaksanakan oleh konstituen Tim Tanggap Insiden Siber;

19) memitigasi kerentanan yang ditemukan baik dari sistem *monitoring* dan pelaporan kerentanan untuk mencegah eksploitasi;

20) menerapkan *patch* atau solusi keamanan lain berdasarkan rencana tanggap insiden kerentanan dan *best practices*; dan

21) menyusun dan mendokumentasikan laporan respons kerentanan.

6. Unit Tata Kelola : 1) menyusun, memelihara, dan mengevaluasi dokumen kebijakan, standar, dan prosedur pengelolaan insiden siber pada organisasi Tim Tanggap Insiden Siber; dan

2) membuat dan melaksanakan program edukasi kesadaran keamanan siber.

7. Unit Komunikasi dan Informasi : 1) membuat dan menjalankan strategi komunikasi terkait keamanan siber;

2) melakukan evaluasi komunikasi terkait strategi komunikasi terkait keamanan siber; dan

		3)	membuat publikasi terkait dengan *best practices* proses tanggap Insiden Siber.
8. Agen Penanganan Insiden Siber	:	1)	melakukan *monitoring* sistem elektronik pada masing-masing perangkat daerah dan melaporkan kejadian insiden siber yang terjadi;
		2)	memperbaiki atau memitigasi kerentanan yang ditemukan baik dari sistem *monitoring* dan pelaporan kerentanan untuk mencegah eksploitasi;
		3)	mengidentifikasi, dan mendokumentasikan kebutuhan kompetensi SDM terkait keamanan siber; dan
		4)	melaksanakan fungsi sebagai narahubung terkait pengelolaan insiden siber.

SEKRETARIS DAERAH PROVINSI DAERAH KHUSUS
IBUKOTA JAKARTA,

MARULLAH MATALI
NIP 196511271996031003