KEPUTUSAN BUPATI KERINCI

NOMOR : 118 /Kep.Bup/2025

TENTANG

PEMBENTUKAN TIM TANGGAP INSIDEN SIBER

COMPUTER SECURITY INCIDENT RESPON TEAM KABUPATEN KERINCI

(KERINCIKAB-CSIRT)

BUPATI KERINCI

Menimbang : a. bahwa pemanfaatan teknologi informasi dan komunikasi (TIK) maupun teknologi terkait dapat menyebabkan kerawanan dan ancaman siber yang meliputi aspek kerahasiaan, keutuhan, ketersediaan, nirsangkal, otentisitas, dan akuntabilitas, 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 - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT);

e. bahwa untuk memenuhi maksud pada huruf a, b, c dan d, dipandang perlu menetapkan Keputusan Bupati tentang Penetapan Pembentukan Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-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. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 238) menjadi Undang-Undang;
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) Pasal 40 dan 41 (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber;
5. Peraturan Daerah Kabupaten Kerinci Nomor 5 Tahun 2022 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Kerinci Tahun 2022 Nomor 5);
6. Peraturan Bupati Kabupaten Kerinci Nomor 2 Tahun 2023 tentang Organisasi dan Tata Kerja Perangkat Daerah (Berita Daerah Kabupaten Kerinci Tahun 2023)
7. Peraturan Bupati Kerinci Nomor 12 Tahun 2024 tentang Sistem Pemerintahan Berbasis Elektronik.

MEMUTUSKAN:

Menetapkan :

KESATU : Membentuk Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT).

KEDUA : Susunan keanggotaan Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) sebagaimana dimaksud diktum kesatu tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan ini.

KETIGA : Tim Tanggap Insiden Siber- *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) mempunyai layanan penanganan insiden siber, berupa:

a. penanggulangan dan pemulihan Insiden Siber;
b. penyampaian informasi Insiden Siber kepada pihak terkait; dan
c. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber

KEEMPAT : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) memiliki fungsi Utama berupa:

a. pemberian peringatan terkait Keamanan Siber;
b. perumusan panduan teknis penanganan Insiden Siber;
c. pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
d. pemilahan (*triage*) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;
e. penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan
f. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.

Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) memiliki fungsi lainnya berupa:

a. penanganan kerentanan Sistem Elektronik;
b. penanganan artefak digital;
c. pemberitahuan hasil pengamatan potensi ancaman;
d. pendeteksian serangan;
e. analisis risiko Keamanan Siber; dan
f. konsultasi terkait kesiapan penanganan Insiden Siber.

KELIMA : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) memiliki konstituen yaitu Perangkat Daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Kerinci.

KEENAM : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) sebagaimana dimaksud dalam Diktum Kesatu mempunyai tugas dan tanggung jawab sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan ini.

KETUJUH : Untuk kelancaran pelaksanaan tugas Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) dapat berkoordinasi dan bekerja sama dengan pihak-pihak lain.

KEDELAPAN : Membebankan biaya pelaksanaan tugas Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Kerinci (Kerincikab-CSIRT) ini pada Anggaran Pendapatan dan Belanja Daerah Kabupaten Kerinci di Dinas Komunikasi dan Informatika Kabupaten Kerinci.

KESEMBILAN : Keputusan Bupati Kerinci ini berlaku sejak tanggal ditetapkan.

Ditetapkan di Siulak
Pada tanggal 13 Juni 2025

BUPATI KERINCI

MONADI

Tembusan disampaikan kepada Yth:

1. Ketua DPRD Kab. Kerinci di Ujung Ladang;
2. Inspektur Pemerintah Kab. Kerinci di Siulak;
3. Kepala Bagian Hukum Setda Kab. Kerinci di Siulak;
4. Yang bersangkutan;

LAMPIRAN KEPUTUSAN BUPATI KERINCI
NOMOR : 118 /Kep.Bup/2025
TENTANG PEMBENTUKAN TIM TANGGAP INSIDEN SIBER - *COMPUTER SECURITY INCIDENT RESPON TEAM* KABUPATEN KERINCI (KERNCIKAB-CSIRT)

SUSUNAN, TUGAS DAN TANGGUNG JAWAB
COMPUTER SECURITY INCIDENT RESPONSE TEAM
KABUPATEN KERINCI (KERINCIKAB-CSIRT)

NO.	JABATAN / FUNGSI DALAM TIM	JABATAN DALAM INSTANSI	URAIAN TUGAS DAN TANGGUNG JAWAB
A.	Pengarah		
	1. Ketua	Bupati Kerinci	1. menjamin terselenggaranya pengelolaan penanggulangan dan pemulihan insiden siber yang meliputi organisasi, sumber daya manusia, dan anggaran yang memadai; dan 2. memberikan pembinaan, kebijakan, sasaran, dan petunjuk teknis dalam penyelenggaraan pengelolaan pengaduan pelayanan insiden siber.
	2. Wakil Ketua	Wakil Bupati Kerinci	1. memberikan masukan kepada Ketua untuk menjamin terselenggaranya pengelolaan insiden siber meliputi organisasi, sumber daya manusia, dan anggaran yang memadai; 2. membantu memberikan pembinaan, kebijakan, dan petunjuk teknis dalam pengelolaan penanggulangan, dan pemulihan insiden siber; dan 3. membantu Ketua dalam melaksanakan tugas dan tanggung jawabnya.

	3. Anggota	1. Sekretaris Daerah Kabupaten Kerinci 2. Asisten Sekretaris Daerah Bidang Pemerintahan dan Kesra Setda Kerinci.	1. memberikan masukan terhadap tujuan, sasaran, dan kegiatan pengelolaan penanggulangan dan pemulihan insiden siber; 2. memberikan masukan terhadap pelaksanaan teknis pengelolaan penanggulangan dan pemulihan insiden siber; 3. menyiapkan dukungan teknis operasional yang diperlukan oleh tim pelaksana; dan 4. melaksanakan tugas terkait pengelolaan penanggulangan dan pemulihan insiden siber yang diberikan oleh Ketua Pengarah.
B.	Pelaksana		
	1. Ketua	Kepala Dinas Komunikasi dan Informatika Kabupaten Kerinci	1. memimpin pelaksanaan tugas CSIRT dalam melakukan pembinaan, pengendalian, pengelolaan, dan pengawasan evaluasi terhadap operasi dan kendali serta personil; dan 2. bertanggung jawab atas pelaksanaan operasional CSIRT.
	2. Sekretaris	Sekretaris Dinas Komunikasi dan Informatika	1. administrasi yang efisien, perencanaan organisasi, dan pengelolaan dokumentasi organisasi CSIRT; 2. menyusun, memelihara, dan mengevaluasi dokumen kebijakan, standar, dan prosedur keamanan informasi pada organisasi CSIRT; 3. menyusun metrik pengukuran tingkat kematangan penerapan keamanan informasi pada organisasi CSIRT; dan 4. menyusun metrik pengukuran evaluasi tingkat kematangan dan kinerja organisasi CSIRT; 5. melaksanakan evaluasi rutin terhadap pelaksanaan program dan kegiatan Kerincikab-CSIRT.
	3. Unit *Monitoring,* Aksi, Penanganan Kerentanan dan Pembinaan	Kepala Bidang Layanan e-Government	1. melakukan perencanaan, pengawasan, dan evaluasi terhadap operasional monitoring tanggap Insiden Siber, dan uji penetrasi sistem; 2. melakukan perencanaan, pelaksanaan, pengawasan dan evaluasi terhadap penelitian kerentanan, penerimaan

			laporan kerentanan, analisis kerentanan, koordinasi dan pengungkapan kerentanan, dan respons kerentanan; dan 3. melakukan perencanaan, pelaksanaan, pengawasan dan evaluasi terhadap berbagi informasi, peningkatan kesadaran keamanan siber, dan pelatihan keamanan siber.
	3.1. Fungsi monitoring, Tanggap Insiden Siber dan Uji Penetrasi		
	a. Koordinator	Pranata Komputer Ahli Muda Dinas Komunikasi dan Informatika	1. melakukan pemantauan terhadap jaringan, sistem, dan aplikasi untuk mendeteksi aktivitas yang mencurigakan atau anomali; 2. menggunakan alat pemantauan jaringan dan sistem seperti SIEM (*Security Information and Event Management*), IDS/IPS (*Intrusion Detection/ Prevention Systems*), dan alat pemantauan log; 3. menganalisis log sistem dan peristiwa keamanan untuk mengidentifikasi tanda-tanda kompromi atau serangan; 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. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan monitoring. 8. membuat, memelihara dan mengevaluasi standar operasional dan prosedur proses tanggap Insiden Siber; 9. memberikan asistensi dan/atau bantuan terkait tanggap Insiden Siber kepada konstituen CSIRT; 10. melakukan pemilahan (*triage*) Insiden Siber sesuai kriteria yang ditetapkan; 11. melakukan penanganan artefak digital;
	b. Anggota	Personil pada Bidang Layanan e-Government	

			12. melakukan akuisisi dan preservasi data dan informasi yang diperlukan dalam proses investigasi atau tanggap Insiden Siber; 13. Membuat laporan proses tanggap Insiden Siber yang dilakukan; 14. melakukan pengelolaan, pendokumentasi-an terhadap laporan tanggap Insiden Siber; 15. membuat publikasi terkait dengan best practices proses tanggap Insiden Siber; 16. 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 CSIRT dan forum berbagi koordinasi dan komunikasi CSIRT; 17. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan tanggap insiden;
			18. melakukan pemindaian kerentanan secara berkala terhadap aset konstituen CSIRT; 19. mengidentifikasi kerentanan dalam sistem; 20. menilai dampak potensial dari kerentanan; 21. melakukan penanganan kerentanan sistem elektronik; 22. menyusun laporan kerentanan secara berkala berdasarkan konstituen CSIRT; 23. melakukan reviu terhadap laporan kerentanan; dan 24. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan uji penetrasi.
	3.2. Fungsi Analisis Kerentanan, Penerima Laporan Kerentanan dan Pengungkapan Kerentanan		
	a. Koordinator	Pranata Komputer Ahli Muda Dinas Komunikasi dan	1. mengidentifikasi kerentanan yang dieksploitasi dan laporan kerentanan sebagai bagian dari insiden keamanan;

		Informatika	2. mempelajari kerentanan baru dengan membaca sumber publik atau sumber pihak ketiga lainnya; 3. menemukan atau mencari kerentanan baru sebagai akibat dari aktivitas atau penelitian yang disengaja; 4. melakukan analisis tren dari *feed* dan data kerentanan dikumpulkan, untuk memahami konstituen atau TTP aktor serangan; 5. membuat perencanaan, pengelolaan dan evaluasi kegiatan pada bagian teknis penelitian dan pelaporan kerentanan; 6. melakukan pemindaian kerentanan secara berkala terhadap aset konstituen CSIRT; 7. melakukan pengumpulan, pengolahan, dan analisis kerentanan keamanan siber lainnya yang mencakup ancaman, kerentanan, dan produk/perangkat TI; 8. menyusun rekomendasi dan laporan kerentanan secara berkala;
	b. Anggota	Personil pada Bidang Layanan e-Government	
			9. melakukan reviu terhadap laporan kerentanan; 10. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan analisis kerentanan; 11. memastikan pemberitahuan informasi kerentanan tepat waktu dan terdistribusi yang akurat; 12. menjaga arus informasi dan melacak status aktivitas entitas yang ditugaskan atau diminta untuk berpartisipasi dalam merespons insiden keamanan informasi; 13. memastikan rekomendasi kerentanan dilaksanakan oleh konstituen CSIRT; 14. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan koordinasi dan pengungkapan kerentanan; 15. memperbaiki atau memitigasi kerentanan yang ditemukan baik dari sistem monitoring dan pelaporan kerentanan untuk

			mencegah eksploitasi; 16. menerapkan patch atau solusi keamanan lain berdasarkan rencana tanggap insiden kerentanan dan *best preactice*; 17. menyusun dan mendokumentasikan laporan respons kerentanan; dan 18. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan respons kerentanan 19. menyusun dan mendokumentasikan laporan respons kerentanan; dan 20. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan respons kerentanan
	3.3. Fungsi Peningkatan Kesadaran Keamanan Siber dan Fungsi Pelatihan Keamanan Siber		
	a. Koordinator	Pranata Komputer Ahli Muda Dinas Komunikasi dan Informatika	1. membuat strategi komunikasi untuk membangun berbagi informasi keamanan siber; 2. mengelola akun media sosial terkait dengan publikasi CSIRT; 3. mengelola portal publikasi terkait dengan publikasi CSIRT; 4. memperhitungkan audiens saat informasi dibuat dan disebarluaskan; 5. menerima masukan, laporan, komentar, dan pertanyaan dari konstituen CSIRT; 6. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan berbagi informasi; 7. membuat dan melaksanakan program edukasi keamanan siber; 8. membuat laporan publikasi mengenai kondisi terkini keamanan siber organisasi (laporan bulanan, laporan 3 bulanan, laporan 6 bulanan, dan laporan tahunan); 9. membuat publikasi teknis mengenai keamanan siber;
	b. Anggota	Personil pada Bidang Layanan e-Government	

			10. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan peningkatan kesadaran keamanan siber; 11. membuat dan melaksanakan program pelatihan keamanan siber; 12. memberikan pelatihan dan pendidikan keamanan siber kepada konstituen CSIRT (yang mungkin mencakup staf organisasi dan CSIRT); 13. menilai, mengidentifikasi, dan mendo-kumentasikan kebutuhan kompetensi SDM untuk mengembangkan materi pelatihan dan pendidikan yang sesuai dan meningkatkan tingkat keterampilannya; dan 14. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan pelatihan keamanan siber
	Agen Penanganan Insiden Siber	Perwakilan Pengelola Sistem Elektronik pada Perangkat Daerah di lingkungan Pemerintah Kabupaten Kerinci	Melakukan monitoring sistem elektronik pada masing-masing perangkat daerah dan melaporkan kejadian insiden siber yang terjadi kepada koordinator.

BUPATI KERINCI

MONADI