BUPATI TRENGGALEK

PROVINSI JAWA TIMUR

KEPUTUSAN BUPATI TRENGGALEK

NOMOR : 100.3.3.2/ 236 /406.001.3/2025

TENTANG

TIM TANGGAP INSIDEN SIBER

COMPUTER SECURITY INCIDENT RESPON TEAM

KABUPATEN TRENGGALEK (Trenggalekkab-CSIRT)

BUPATI TRENGGALEK,

Menimbang : a. bahwa pemanfaatan teknologi informasi dan komunikasi (TIK) maupun teknologi terkait dapat menyebabkan kerawanan dan ancaman siber yang meliputi aspek kerahasiaan, keutuhan, ketersediaan, nir-sangkal, 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 berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Keputusan Bupati Trenggalek tentang Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab-CSIRT);

Mengingat : 1. Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Provinsi Jawa Timur (Lembaran Negara Republik Indonesia Tahun 1950 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 9) sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 tentang Perubahan Batas Wilayah Kotapraja Surabaya dan Daerah Tingkat II Surabaya dengan mengubah Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Provinsi Jawa Timur dan Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar dalam Lingkungan Provinsi Jawa Timur, Jawa Tengah, Jawa Barat dan Daerah Istimewa Jogjakarta (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 2730);

2. 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);
3. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);
4. 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 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 Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);

5. Undang-Undang Nomor 12 Tahun 2023 tentang Provinsi Jawa Timur (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 59, Tambahan Lembaran Negara Republik Indonesia Nomor 6868);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 157);
8. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
9. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 8 Tahun 2019 tentang Penyelenggaraan Urusan Pemerintahan Konkuren Bidang Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2019 Nomor 1026);
10. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
11. Peraturan Badan Siber dan Sandi Negara Republik Indonesia Nomor 1 Tahun 2024 tentang Pengelolaan

Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);

12. Peraturan Bupati Trenggalek Nomor 11 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintah Berbasis Elektronik di Lingkungan Pemerintah Daerah (Berita Daerah Kabupaten Trenggalek Tahun 2022 Nomor 11);

MEMUTUSKAN:

Menetapkan :

KESATU : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab-CSIRT) dengan susunan keanggotaan sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan Bupati ini.

KEDUA : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab-CSIRT) sebagaimana dimaksud pada DIKTUM KESATU Keputusan Bupati ini mempunyai layanan penanganan insiden siber, berupa:

1. penanggulangan dan pemulihan insiden siber;
2. penyampaian informasi insiden siber kepada pihak terkait; dan
3. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari insiden siber.

KETIGA : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab-CSIRT) sebagaimana dimaksud pada DIKTUM KESATU Keputusan Bupati ini memiliki fungsi utama berupa:

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 : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab CSIRT) sebagaimana dimaksud pada DIKTUM KESATU Keputusan Bupati ini memiliki fungsi lainnya berupa:

1. penanganan kerentanan sistem elektronik;
2. pemberitahuan hasil pengamatan potensi ancaman;
3. pendeteksian serangan;
4. analisis risiko keamanan siber; dan
5. konsultasi terkait kesiapan penanganan insiden siber.

KELIMA : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab-CSIRT) sebagaimana dimaksud pada DIKTUM KESATU Keputusan Bupati ini memiliki konstituen yaitu Perangkat Daerah penyelenggara sistem elektronik di lingkungan Pemerintah Kabupaten Trenggalek.

KEENAM : Tim Tanggap Insiden Siber - *Computer Security Incident Respon Team* Kabupaten Trenggalek (Trenggalekkab-CSIRT) sebagaimana dimaksud pada DIKTUM KESATU Keputusan Bupati ini mempunyai tugas dan tanggung jawab sebagaimana tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Keputusan Bupati ini.

KETUJUH : Untuk kelancaran pelaksanaan tugas Trenggalekkab-CSIRT dapat berkoordinasi dan bekerja sama dengan pihak-pihak lain.

KEDELAPAN : Segala biaya yang diperlukan untuk pelaksanaan tugas Trenggalekkab-CSIRT dibebankan pada Anggaran Pendapatan dan Belanja Daerah Kabupaten Trenggalek tahun berkenaan.

KESEMBILAN : Keputusan Bupati ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Trenggalek
pada tanggal 13 Juni 2025

BUPATI TRENGGALEK,

MOCHAMAD NUR ARIFIN

LAMPIRAN
KEPUTUSAN BUPATI TRENGGALEK
NOMOR : 100.3.3.2/ 236 /406.001.3/2025
TENTANG TIM TANGGAP INSIDEN SIBER - *COMPUTER SECURITY INCIDENT RESPON TEAM* KABUPATEN TRENGGALEK (Trenggalekkab-CSIRT)

SUSUNAN KEANGGOTAAN, TUGAS DAN TANGGUNG JAWAB TIM TANGGAP INSIDEN SIBER-
COMPUTER SECURITY INCIDENT RESPONSE TEAM
KABUPATEN TRENGGALEK (Trenggalekkab-CSIRT)

NO.	JABATAN / FUNGSI DALAM TIM	JABATAN DALAM INSTANSI	URAIAN TUGAS DAN TANGGUNG JAWAB
A.	**Pengarah**		
	1. Ketua	Bupati Trenggalek	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	Sekretaris Daerah Kabupaten Trenggalek	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	Asisten Administrasi Umum Sekda Kabupaten Trenggalek	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 Trenggalek	1. memimpin pelaksanaan tugas TTIS dalam melakukan pembinaan, pengendalian, pengelolaan, dan pengawasan evaluasi terhadap operasi dan kendali serta personil; 2. bertanggung jawab atas pelaksanaan operasional TTIS
	2. Sekretaris	Sekretaris Dinas Komunikasi dan Informatika Kabupaten Trenggalek	1. administrasi yang efisien, perencanaan organisasi, dan pengelolaan dokumentasi organisasi TTIS; 2. menyusun, memelihara, dan mengevaluasi dokumen kebijakan, standar, dan prosedur keamanan informasi pada organisasi TTIS; 3. menyusun metrik pengukuran tingkat kematangan penerapan keamanan informasi pada organisasi TTIS; dan 4. menyusun metrik pengukuran evaluasi tingkat kematangan dan kinerja organisasi TTIS; 5. melaksanakan evaluasi rutin terhadap pelaksanaan program dan kegiatan Trenggalekkab-CSIRT

	3. Unit Monitoring dan Aksi	Kepala Bidang Statistik dan Persandian Kabupaten Trenggalek	melakukan perencanaan, pengawasan, dan evaluasi terhadap operasional monitoring tanggap Insiden Siber, dan uji penetrasi sistem
	3.1. Fungsi Monitoring		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	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; dan 7. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan monitoring
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika 2. Pranata Komputer pada Bidang Statistik dan Persandian	
	3.2. Fungsi Tanggap Insiden		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. membuat, memelihara dan mengevaluasi standar operasional dan prosedur proses tanggap Insiden Siber; 2. memberikan asistensi dan/atau bantuan terkait tanggap Insiden Siber kepada konstituen TTIS; 3. melakukan pemilahan (triage) Insiden Siber sesuai kriteria yang ditetapkan; 4. melakukan penanganan artefak digital;
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika 2. Pranata Komputer pada Bidang Statistik dan Persandian	

			5. melakukan akuisisi dan preservasi data dan informasi yang diperlukan dalam proses investigasi atau tanggap Insiden Siber; 6. Membuat laporan proses tanggap Insiden Siber yang dilakukan; 7. melakukan pengelolaan, pendokumentasi-an terhadap laporan tanggap Insiden Siber; 8. membuat publikasi terkait dengan best practices proses tanggap Insiden Siber; 9. 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; dan 10. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan tanggap insiden
	3.3. Fungsi Uji Penetrasi		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. melakukan pemindaian kerentanan secara berkala terhadap aset konstituen TTIS; 2. mengidentifikasi kerentanan dalam sistem; 3. menilai dampak potensial dari kerentanan; 4. melakukan penanganan kerentanan sistem elektronik; 5. menyusun laporan kerentanan secara berkala berdasarkan konstituen TTIS; 6. melakukan reviu terhadap laporan kerentanan; dan 7. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan uji penetrasi
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika 2. Pranata Komputer pada Bidang Statistik dan Persandian	
	4. Unit Penanganan Kerentanan	Kepala Bidang Aplikasi Informatika	melakukan perencanaan, pelaksanaan, pengawasan dan evaluasi terhadap penelitian kerentanan, penerimaan laporan kerentanan, analisis kerentanan,

			koordinasi dan pengungkapan kerentanan, dan respons kerentanan
	4.1. Fungsi Peneliti dan Penerima Laporan Kerentanan		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. mengidentifikasi kerentanan yang dieksploitasi dan laporan kerentanan sebagai bagian dari insiden keamanan; 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; dan 5. membuat perencanaan, pengelolaan dan evaluasi kegiatan pada bagian teknis penelitian dan pelaporan kerentanan
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika 2. Pranata Komputer pada Bidang Statistik dan Persandian	
	4.2. Fungsi Analisis Kerentanan		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. melakukan pemindaian kerentanan secara berkala terhadap aset konstituen TTIS; 2. melakukan pengumpulan, pengolahan, dan analisis kerentanan keamanan siber lainnya yang mencakup ancaman, kerentanan, dan produk/perangkat TI; 3. menyusun rekomendasi dan laporan kerentanan secara berkala; 4. melakukan reviu terhadap laporan kerentanan; dan 5. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan analisis kerentanan
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika 2. Pranata Komputer pada Bidang Statistik dan Persandian	
	4.3. Fungsi Koordinasi dan Pengungkapan Kerentanan		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. memastikan pemberitahuan informasi kerentanan tepat waktu dan terdistribusi yang akurat; 2. menjaga arus informasi dan melacak status aktivitas entitas yang ditugaskan atau diminta untuk
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika	

		2. Pranata Komputer pada Bidang Statistik dan Persandian	berpartisipasi dalam merespons insiden keamanan informasi; 3. memastikan rekomendasi kerentanan dilaksanakan oleh konstituen TTIS; dan 4. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan koordinasi dan pengungkapan kerentanan
	4.4. Fungsi Respons Kerentanan		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. memperbaiki atau memitigasi kerentanan yang ditemukan baik dari sistem monitoring dan pelaporan kerentanan untuk mencegah eksploitasi; 2. menerapkan patch atau solusi keamanan lain berdasarkan rencana tanggap insiden kerentanan dan best preactice; 3. menyusun dan mendokumentasikan laporan respons kerentanan; dan 4. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan respons kerentanan
	b. Anggota	1. Pranata Komputer pada Bidang Aplikasi Informatika 2. Pranata Komputer pada Bidang Statistik dan Persandian	
	5. Unit Pembinaan dan Publikasi	Kepala Bidang Statistik dan Persandian	melakukan perencanaan, pelaksanaan, pengawasan dan evaluasi terhadap berbagi informasi, peningkatan kesadaran keamanan siber, dan pelatihan keamanan siber
	5.1. Fungsi Berbagi Informasi		
	a. Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. membuat strategi komunikasi untuk membangun berbagi informasi keamanan siber; 2. mengelola akun media sosial terkait dengan publikasi TTIS; 3. mengelola portal publikasi terkait dengan publikasi TTIS; 4. memperhitungkan audiens y saat informasi dibuat dan disebarluaskan;
	b. Anggota	Personil pada Seksi Persandian dan Keamanan Informasi	

			5. menerima masukan, laporan, komentar, dan pertanyaan dari konstituen TTIS; dan 6. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan berbagi informasi
	5.2. Fungsi Peningkatan Kesadaran Keamanan Siber		
	Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. membuat dan melaksanakan program edukasi keamanan siber; 2. membuat laporan publikasi mengenai kondisi terkini keamanan siber organisasi (laporan bulanan, laporan 3 bulanan, laporan 6 bulanan, dan laporan tahunan); 3. membuat publikasi teknis mengenai keamanan siber; 4. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan peningkatan kesadaran keamanan siber
	Anggota	Personil pada Seksi Persandian dan Keamanan Informasi	
	5.3. Fungsi Pelatihan Keamanan Siber		
	Koordinator	Kepala Seksi Persandian dan Kemananan Informasi	1. membuat dan melaksanakan program pelatihan keamanan siber; 2. memberikan pelatihan dan pendidikan keamanan siber kepada konstituen TTIS (yang mungkin mencakup staf organisasi dan TTIS); 3. menilai, mengidentifikasi, dan mendo-kumentasikan kebutuhan kompetensi SDM untuk mengembangkan materi pelatihan dan pendidikan yang sesuai dan meningkatkan tingkat keterampilannya; dan 4. melakukan pengelolaan terhadap sistem elektronik yang digunakan dalam kegiatan pelatihan keamanan siber
	Anggota	Personil pada Seksi Persandian dan Keamanan Informasi	

	6. Agen Penanganan Insiden Siber	Anggota Tim Admin Website Perangkat Daerah pada Pemerintah Kabupaten Trenggalek	Melakukan monitoring sistem elektronik pada masing-masing perangkat daerah dan melaporkan kejadian insiden siber yang terjadi kepada koordinator

BUPATI TRENGGALEK,

MOCHAMAD NUR ARIFIN