STANDAR OPERASIONAL PROSEDUR PENANGANAN INSIDEN SIBER

2026

PEMERINTAH KABUPATEN TEMANGGUNG
DINAS KOMUNIKASI DAN INFORMATIKA

Alamat : Jl. Jenderal Sudirman No.42 No. 41, Dongkelan Selatan, Jampiroso, Temanggung, Jawa Tengah 56212 Telepon (0293) 496 1389 Faximili 496 1995

PEMERINTAH KABUPATEN TEMANGGUNG
DINAS KOMUNIKASI DAN INFORMATIKA
BIDANG STATISTIK DAN PERSANDIAN

Nomor SOP	:	555/4/2026
Tanggal Pembuatan	:	27 Maret 2026
Tanggal Revisi	:	27 Maret 2026
Tanggal Efektif	:	27 Maret 2026
Disahkan oleh	:	**KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN TEMANGGUNG** **Gotri Winanto Wuriatmojo, S.STP., M.Si.** NIP. 197712121997031006
Nama SOP	:	Penanganan Inseiden Siber

Dasar Hukum	**Kualifikasi Pelaksana**
1 Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43) 2 Peraturan Bupati Temanggung Nomor 31 Tahun 2025 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik 3 Peraturan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia Nomor 1 tahun 2025 tentang Pedoman Pembentukan Tim Tanggap Insiden Siber	1 Memiliki pengetahuan dan ketrampilan bidang jaringan dan *server* 2 Memiliki pengetahuan dan ketrampilan dalam bidang network traffic monitoring 3 Memiliki pengetahuan dalam mengoperasikan perangkat komputer dan server
Keterkaitan SOP	**Peralatan/ Perlengkapan**
1 SOP Maintenance Gangguan Jaringan 2 SOP Penarikan Server dari Data Center 3 SOP Pemeliharaan Server	1 Komputer/Laptop 2 Jaringan Internet 3 Virtual Private Network (VPN) 4 Alat komunikasi 5 Panduan teknis penanganan insiden siber
Peringatan	**Pencatatan & Pendataan**
Apabila SOP ini tidak dilaksanakan maka akan menyebabkan setiap kegiatan menjadi tidak memiliki standar, dan akan menghambat proses kegiatan organisasi secara keseluruhan	1 Dalam SOP ini ada 6 tahapan penanganan insiden siber antara lain: 1. Persiapan 2. Identifikasi/ deteksi 3. Verifikasi 4. Isolasi 5. Pemulihan 6. Evaluasi

No.	KEGIATAN			MUTU BAKU			Keterangan
		CSIRT	TIK	Kelengkapan	Waktu	Output	
1	Tim CSIRT mendapatkan laporan publik terjadinya insiden atau tim CSIRT mendapatkan notifikasi dari sensor yang terpasang			Perangkat sensor, surat elektronik, komputer	15 menit	Laporan publik atau notifikasi insiden siber	
2	Tim CSIRT melakukan verifikasi terhadap laporan atau notifikasi yang didapatkan. Apabila laporan atau notifikasi yang diterima tidak valid, maka laporan tidak ditindaklanjuti	TIDAK YA		Komputer, Laporan Insiden	60 Menit	Hasil verifikasi laporan atau noitifkasi	
3	Apabila laporan atau notifikasi yang diterima valid, laporan diteruskan kepada Bidang TIK untuk ditindaklanjuti			Komputer, Hasil verifiaksi	15 Menit	Laporan insiden	
4	Melakukan isolasi terhadap sistem/ perangkat (*software* maupun *hardware*) yang terinfeksi agar tidak terjadi eskalasi lanjutan			Komputer, Laporan insiden, VPN	60 menit	Laporan Tindak Lanjut	
5	Melakukan analisa dan perbaikan terhadap sistem/perangkat serta menutup celah kerawanan tersebut			Komputer, laporan terkait	2 hari kerja	Laporan Tindak Lanjut	
6	melakukan uji coba terhadap sistem/perangkat yang telah diperbaiki, apakah layak operasional.	TIDAK YA		Komputer, laporan terkait	1 Hari kerja	Laporan Hasil Pengujian	
7	Jika perangkat/sistem layak beroperasi, Bidang TIK melakukan *onboarding* perangkat/sistem.			Komputer, laporan hasil pengujian	120 Menit	Berita Acara Penganan Insiden Siber	
8	Membuat laporan penanganan/pasca insiden serta Dilakukan pembelajaran agar tidak terjadi insiden serupa dikemudian			Komputer, Berita Acara Penanganan Insiden Siber	60 menit	Laporan Penanganan/ Pasca Insiden Siber	