PEMERINTAH DAERAH KABUPATEN CIAMIS **DINAS KOMUNIKASI DAN INFORMATIKA**	NOMOR SOP	000.8.3.3/281/Diskominfo.05/2026
	TGL PEMBUATAN	26 Januari 2026
	TGL REVISI	
	TGL EFEKTIF	
	DISAHKAN OLEH	Ditandatangani secara elektronik oleh: KEPALA DINAS KOMUNIKASI DAN INFORMATIKA ENDA HIDAYAT, S.STP., M.Si. NIP. 198309122002121007
BIDANG PERSANDIAN DAN KEAMANAN INFORMASI	NAMA SOP	**PELAPORAN INSIDEN SIBER MASYARAKAT**

DASAR HUKUM	KUALIFIKASI PELAKSANA
1. Undang-undang Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik; 2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 35 Tahun 2012 tentang penyusunan SOP Administrasi Pemerintahan; 3. Peraturan BSSN Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah; 4. Peraturan BSSN Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber; 5. Peraturan BSSN Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik; 6. Peraturan BSSN Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber; 7. Peraturan Bupati Ciamis Nomor 49 Tahun 2016 Tentang Tugas, Fungsi Dan Tata Kerja Dinas Komunikasi Dan Informatika Kabupaten Ciamis; 8. Keputusan Bupati Ciamis Nomor 500.12.1/Kpts.23-Huk/Tahun 2024 tentang Tim Tanggap Insiden Siber Kabupaten Ciamis;	1. Memiliki kemampuan koordinasi dengan pihak terkait. 2. Memiliki kemampuan dalam mengoperasionalkan sistem ticketing. 3. Memiliki kemampuan melakukan pengamanan siber. 4. Memiliki kemampuan analisis dalam mengindentifikasi penyebab insiden siber. 5. Memiliki kemampuan teknis dalam operasional server, jaringan dan instrumen (Tools) Keamanan Siber. 6. Memiliki kemampuan koordinasi dengan baik kepihak terkait. 7. Memahami prinsip – prinsip keamanan informas.

KETERKAITAN	PERALATAN / PERLENGKAPAN
1. SOP Penanganan Insiden Siber. 2. SOP Pelaporan Insiden Siber. 3. SOP Security Patching.	1. Laporan Insiden, Disposisi. 2. Komputer. 3. Jaringan Internet. 4. Tools (Keamanan Siber) Perangkat Komputer. 5. Sistem Ticket. 6. Alat Tulis Kantor dan Media Komunikasi. 7. Dasboard Website : csirt.ciamiskab.go.id. 8. Dashboard Manajemen Tiket
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Apabila prosedur ini dilaksanakan, aplikasi yang berjalan di server akan terpantau dan dapat ditindaklanjuti secara cepat ketika terjadi insiden maupun serangan siber. 2. Apa bila prosedur ini tidak dilaksanakan, aplikasi menjadi sasaran insiden maupun serangan siber tidak dapat segera diperbaiki dan bias menjadi celah keamanan yang lebih besar mengancam aplikasi – aplikasi lain yang berada dalam satu server dengan aplikasi tersebut. 3. Apa bila prosedur ini dilaksanakan oleh pihak – pihak atau individu yang tidak memiliki kompetensi yang disebutkan, proses pelaporan dan penanganan insiden siber tidak akan berjalan dengan baik, karena aspek – aspek yang mungkin harus dilaporakan, dianalisis, diperabaiki, dan diperbaharui tidak terindentifikasi secara lengkap.	1. Ticketing. 2. Proof Of Concept (PoC) / Dokumentasi Insiden. 3. Laporan analisis penyebab insiden dan rekomendasi penanganan insiden siber. 4. Logbook keamanan siber.

URAIAN PROSEDUR PELAPORAN INSIDEN SIBER (MASYARAKAT)									
No.	Kegiatan	Pelaksana				Mutu Baku			Ket
		Pelapor (Masyarakat)	Ciamiskab-CSIRT	Kepala Bidang Persandian dan Keamanan Informasi	OPD Pemilik Sistem Elektronik (SE)	Kelengkapan	Waktu	Output	
1.	Pelapor menemukan insider siber atau celah keamanan siber pada website Pemerintah Daerah Kabupaten Ciamis							Tangkapan layar website yang ditemukan insiden siber atau tools keamanan siber	
2.	Pelapor dapat melakukan pelaporan insiden siber atau celah keamanan siber pada website atau email ciamiskab csirt					• Data diri pelapor • Bukti insiden siber atau temuan celah keamanan siber		Ticket laporan atau email	• Website ciamiskab-CSIRT: https://csirt.ciamiskab.go.id/ • Email: csirt@ciamiskab.go.id
3.	Ciamiskab-CSIRT melakukan konfirmasi dan verifikasi kebenaran mengenai temuan tersebut.					• Ticket laporan atau email • Data diri pelapor • Bukti insiden siber atau temuan celah keamanan siber	3 Jam	• Balasan ticket laporan atau email	
4.	Ciamiskab-CSIRT melakukan analisis lebih lanjut mengenai temuan tersebut dan membuat laporan hasil analisis serta memberikan rekomendasi perbaikan sistem elektronik yang terdampak.			Tidak		Bukti insiden siber atau temuan celah kemanan siber	1 Hari	Laporan Hasil Analisis	
5.	Kepala Bidang Persandian dan Keamanan Informasi melakukan review laporan hasil analisis. Jika masih ada yang kurang maka laporan harus diperbaiki, dan jika sudah benar maka laporan akan ditandatangani.			Ya		Laporan Hasil Analisis	1 Jam	Laporan Hasil Analisis yang telah ditandatangan	
6.	Kepala Bidang Persandian dan Keamanan Informasi meneruskan laporan hasil analisis tersebut ke OPD Pemilik Sistem Elektronik (SE) untuk ditindaklanjuti.					Laporan Hasil Analisis yang telah ditandatangan			