PEMERINTAH KABUPATEN KUTAI KARTANEGARA
DINAS KOMUNIKASI DAN INFORMATIKA

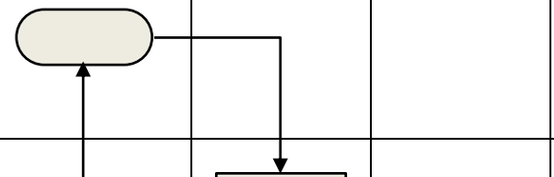
PROSEDUR BAKU PELAKSANAAN KEGIATAN
STANDAR OPERASIONAL PROSEDUR (SOP)

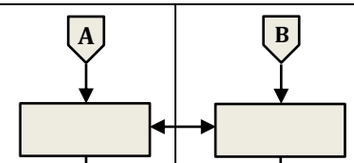
PENANGANAN INSIDEN SIBER

PEMERINTAH KABUPATEN KUTAI KARTANEGARA **DINAS KOMUNIKASI DAN INFORMATIKA**	Nomor SOP	B-247/DISKOMINFO/000.6/07/2025
	Tanggal Pembuatan	10 Juli 2025
	Tanggal Revisi	-
	Tanggal Pengesahan	10 Juli 2025
	Disahkan Oleh	Ditandatangani Secara Elektronik Oleh : Plt. KEPALA DINAS KOMUNIKASI DAN INFORMATIKA **SOLIHIN, S.Sos., M.T.** Pembina Tingkat I
	Nama SOP	Penanganan Insiden Siber

DASAR HUKUM	**KUALIFIKASI PELAKSANA**
1. Peraturan Menteri PAN RB Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan SOP Administrasi Pemerintahan; 2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah; 3. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 Tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik; 4. Peraturan Bupati Kutai Kartanegara Nomor 61 Tahun 2023 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika; 5. Peraturan Bupati Kutai Kartanegara Nomor 34 Tahun 2025 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintah Daerah; 6. Peraturan Bupati Kutai Kartanegara Nomor 36 Tahun 2025 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis	1. Mampu mengoperasikan Komputer dengan baik; 2. Memiliki pengetahuan di bidang keamanan informasi dengan baik; 3. Memiliki kemampuan analisis dalam mengidentifikasi insiden siber; 4. Memiliki kemampuan teknis dalam operasional server, jaringan dan instrument (*tools*) keamanan siber; 5. Memahami prinsip-prinsip keamanan informasi; 6. Memiliki pengetahuan administrasi umum;

Elektronik Di Lingkungan Pemerintah Daerah.	
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
1. SOP Pelaporan Insiden Siber; 2. SOP Monitoring Sistem Elektronik/Aplikasi;	1. Ruang *War Room*; 2. Laporan Insiden, Disposisi; 3. PC/Laptop/Printer; 4. ATK, media komunikasi dan form; 5. Jaringan Internet; 6. *Firewall, Intrusion Detection System/Intrusion Prevention System* (IDS/IPS); 7. Perangkat Lunak *Security Information and Event Management* (SIEM); 8. Perangkat Keras dan Lunak Forensik Digital; 9. Instrumen *Vulnerability Scanning*; 10. *Antivirus & Antimalware;* 11. Software Manajemen Tiket.
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Jika SOP ini tidak berjalan maka akan mengakibatkan dampak yang mencakup keterlambatan perbaikan, peningkatan resiko siber, penurunan efisiensi, rusaknya reputasi organisasi, ketidaksesuaian dengan regulasi dan kerugian finansial; 2. Dapat menyebabkan proses penanganan insiden menjadi tidak terarah; 3. Dapat menyebabkan potensi celah keamanan yang lebih besar; Dapat menghambat pemulihan dan kelancaran oprasional.	1. *Proof of Concepts* (PoC)/Dokumentasi Insiden; 2. Formulir Laporan Insiden 3. Dokumentasi Kegiatan; 4. Laporan Penanganan.

NO.	URAIAN PROSEDUR	PELAKSANA				MUTU BAKU			KETERANGAN
		Pelapor(Tim Monitoring SE/Masyarakat)	Narahubung	TTIS KUKARKAB	CSIRT Provinsi Kaltim/CSIRT Nasional	Kelengkapan	Waktu	Output	
1	Melaporkan temuan Insiden siber					KTP, nomor kontak yang dapat dihubungi, alamat email, bukti laporan (Poc)	30 Menit	Form laporan insiden siber beserta nomor tiket laporan	Dilakukan melalui website ttis.kukarkab.go.id
2	Mencatat dan meneruskan laporan temuan insiden kepada tim tanggap insiden siber								
3	Melakukan verifikasi laporan insiden, bila sesuai laporan akan ditindak lanjut, bila tidak sesuai laporan dikembalikan kepada pelapor		Tidak Sesuai	Sesuai		PC/laptop, printer, jaringan internet, nomor tiket laporan, form laporan insiden	30 Menit	Dokumen laporan insiden siber yang memenuhi syarat yang harus ditangani	Dilakukan melalui rapat tim dan media komunikasi
4	Tim Tanggap Insiden melakukan analysis root cause investigation atas insiden					PC/laptop, jaringan internet, instrumen investigasi	1 Hari	Dokumen analisis insiden siber	Dilaksanakan oleh Tim Tanggap Insiden Siber Kukarkab
5	Menentukan apakah insiden bisa ditangani oleh Tim, bila dianggap insiden skala besar maka akan dikoordinasikan dan ditangani oleh Tim CSIRT Provinsi Kaltim/CSIRT Nasional			Sesuai	Tidak	PC/laptop, jaringan internet, instrumen investigasi	1 Hari	Surat Permohonan Penangan Insiden Siber	Surat Permohonan ditujukan kepada CSIRT Provinsi Kaltim atau CSIRT Nasional Badan Siber dan Sandi Negara
6	Penanganan insiden siber			A	B	PC/laptop, jaringan internet, instrumen investigasi	5 Hari	Dokumentasi kegiatan	Lama penanganan tergantung skala dan kategori insiden siber

7	Melakukan koordinasi antara Tim Tanggap Insiden Siber dengan Tim CSIRT Provinsi Kaltim/CSIRT Nasional					PC/laptop, jaringan internet, instrumen investigasi	2 Hari	Dokumentasi kegiatan, notula	Koordinasi dilakukan antara TTIS Kukarkab dengan CSIRT Provinsi Kaltim/CSIRT Nasional
8	Menyusun laporan hasil penanganan insiden siber					PC/laptop, printer, ATK, jaringan internet,	1 Hari	Dokumen laporan penanganan/investigasi	Disusun berdasarkan hasil rapat tim
9	Menyerahkan hasil laporan kepada narahubung					PC/laptop, jaringan internet, media komunikasi	5 Menit	Dokumen laporan	Laporan berupa dokumen *soft/hard copy*
10	Mengirimkan laporan hasil penanganan insiden siber dan proses dianggap selesai					Dokumen Laporan, sertifikat apresiasi, berita acara serah terima dokumen	5 Menit	BAST Laporan	Laporan dikirimkan kepada Penyelenggara Sistem Elektronik