PEMERINTAH KABUPATEN KUTAI KARTANEGARA
DINAS KOMUNIKASI DAN INFORMATIKA

PROSEDUR BAKU PELAKSANAAN KEGIATAN
STANDAR OPERASIONAL PROSEDUR (SOP)

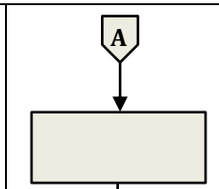
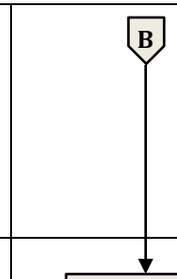
MONITORING SISTEM ELEKTRONIK

PEMERINTAH KABUPATEN KUTAI KARTANEGARA **DINAS KOMUNIKASI DAN INFORMATIKA**	Nomor SOP	B-246/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	Monitoring Sistem Elektronik

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 Elektronik Di Lingkungan Pemerintah Daerah.	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;

KETERKAITAN	PERALATAN/PERLENGKAPAN
1. SOP Pelaporan Insiden Siber; 2. SOP Penanganan Insiden Siber.	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; 4. Dapat menghambat pemulihan dan kelancaran operasional.	1. *Proof of Concepts* (PoC)/Dokumentasi Insiden; 2. Formulir Laporan Insiden 3. Dokumentasi Kegiatan; 4. Daftar Security Log Analysis 5. Laporan Insiden Siber.

NO	URAIAN PROSEDUR	PELAKSANA			MUTU BAKU			KETERANGAN
		TTIS KUKARKAB	KOORDINATOR TIM/KEPALA BIDANG PERSANDIAN	KETUA TIM/KEPALA DINAS	Kelengkapan	Waktu	Output	
1	Login ke aplikasi monitoring (SIEM)				PC/laptop, jaringan internet	5 Menit	Dashboard SIEM	Login ke Forti Client
2	Mengakses *dashboard* apllikasi monitoring (SIEM)				PC/laptop, printer, jaringan internet	5 Menit	Dashboard SIEM	Dashboard aplikasi monitoring (SIEM)
3	Melakukan analisis data keamanan pada daftar *Security Log Analysis*				PC/laptop, jaringan internet, data-data log, media komunikasi	180 Menit	Catatan analisis data log	Mengakses fitur-fitur *security log analysis*, mencai referensi jenis-jenis serangan
4	JIka ditemukan Log Anomali maka dilanjutkan dengan pemeriksaan lebih mendalam pada log tersebut, jika tidak dilakukan analisis ulang		Tidak		PC/laptop, jaringan internet, data-data log, media komunikasi	1 Hari	Hasil analisis data log	Mempelajari bentuk serangan, skema, mitigasi, penanganan dan mencari penyebab insiden dari celah-celah kerentanan yang ditemukan
5	Melakukan *vulnerability Assessment log anomaly* untuk pembuktian FALSE POSITIVE atau FALSE NEGATIVE	Ya			PC/laptop, jaringan internet, instrumen *vulnerability assessment*, media komunikasi	2 Hari	PoC	Menggunakan instrumen VA serta mengumpulkan PoC untuk menentukan FALSE POSITIVE atau FALSE NEGATIVE
6	JIka FALSE NEGATIVE maka buat laporan hasil temuan berupa laporan insiden siber, jika FALSE POSITIVE membuat laporan kerja	False Negative A	False Positive B		PC/laptop, jaringan internet, media komunikasi	1 Hari	Laporan insiden siber	Dilaksanakan berdasarkan hasil keputusan tim tanggap insiden siber

7	Mengirimkan Laporan hasil temuan untuk diverifikasi Koordinator Tim				PC/laptop, jaringan internet, media komunikasi	5 Menit		Dikirim melalui media komunikasi
8	Melakukan verifikasi laporan dan mengirimkan kepada Ketua Tim/Kepala Dinas				PC/laptop, jaringan internet, media komunikasi	5 Menit	Laporan insiden siber yang diverifikasi	Dilakukan dan dikirim melalui media komunikasi
9	Melakukan pengesahan laporan insiden siber				PC/laptop, jaringan internet, media komunikasi	5 Menit	Laporan insiden siber yang telah disahkan	Dilakukan melalui media komunikasi atau melalui PC/laptop
10	Tim Insiden Siber membuat Surat Pemberitahuan kepada PSE, monitoring selesai				PC/laptop, jaringan internet, media komunikasi	10 Menit	Surat pemberitahuan insiden siber	Dilakukan melalui media komunikasi atau melalui PC/laptop