



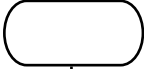
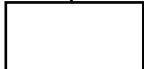
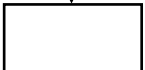
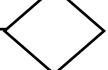
PEMERINTAH KABUPATEN KUTAI KARTANEGARA
DINAS KOMUNIKASI DAN INFORMATIKA

PROSEDUR BAKU PELAKSANAAN KEGIATAN
STANDAR OPERASIONAL PROSEDUR (SOP)

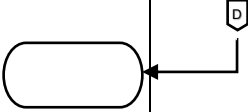
PELAPORAN INSIDEN SIBER KE PIHAK BERWAJIB

 PEMERINTAH KABUPATEN KUTAI KARTANEGARA DINAS KOMUNIKASI DAN INFORMATIKA	Nomor SOP	B-020/DISKOMINFO/000.8.3.3/08/2025
	Tanggal Pembuatan	6 Agustus 2025
	Tanggal Revisi	-
	Tanggal Pengesahan	6 Agustus 2025
	Disahkan Oleh	 Ditandatangani Secara Elektronik Oleh : Plt. KEPALA DINAS KOMUNIKASI DAN INFORMATIKA SOLIHIN, S.Sos., M.T. Pembina Tingkat I
	Nama SOP	Pelaporan Insiden Siber Ke Pihak Berwajib
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 dibidang Keamanan Informasi dengan baik; 3. Memiliki pengetahuan administrasi umum; 4. Memiliki kemampuan analisis dalam mengidentifikasi penyebab insiden siber 5. Memiliki kemampuan teknis dalam operasional server, jaringan dan instrumen (<i>Tools</i>) Keamanan Siber; 6. Memiliki kemampuan koordinasi dengan baik kepihak terkait; 7. Memahami prinsip – prinsip keamanan informasi;

KETERKAITAN	PERALATAN/PERLENGKAPAN
1. SOP Monitoring Sistem Elektronik/Aplikasi; 2. SOP Penanganan Insiden Siber; 3. SOP Pelaporan Insiden Siber; 4. SOP Security Patching.	1. Laporan Insiden, Disposisi; 2. PC/Laptop/Printer; 3. Jaringan Internet; 4. Tools (Keamanan Siber) Perangkat Komputer; 5. Alat Tulis Kantor dan Media Komunikasi; 6. Formulir Permohonan; 7. Dashboard Website : ttis.kukarkab.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 dilaporkan, dianalisis, diperbaiki, dan diperbaharui tidak teridentifikasi secara lengkap.	1. <i>Proof Of Concept (PoC)</i> / Dokumentasi Insiden; 2. Formulir laporan insiden siber; 3. Dokumentasi kegiatan; 4. Laporan analisis penyebab insiden dan rekomendasi penanganan insiden siber. 5. Logbook keamanan siber;

No	URAIAN PROSEDUR	PELAKSANA				MUTU BAKU			KETERANGAN
		Pelapor (Tim Monitoring SE/Masyarakat)	Petugas	TTIS KUKARKAB	Pihak Berwajib	Kelengkapan	Waktu	Output	
1	Proses Laporan Insiden Keamanan dimulai.					- PC/Laptop - Jaringan Internet	5 Menit	Dashboard website ttis.kukarkab.go.id	Dilakukan melalui website ttis.kukarkab.go.id
2	Menerima laporan adanya gangguan atau insiden terkait keamanan informasi, laporan dapat berasal dari pihak luar maupun dari Tim Internal Perangkat Daerah (PD).					- PC/Laptop - Jaringan Internet - Data Pelapor dan Laporan Insiden - Bukti Insiden	10 Menit	Formulir Laporan Insiden	
3	Petugas Mencatat / Menginput Laporan Insiden terkait keamanan informasi berdasarkan informasi yang disampaikan oleh Pelapor.					- PC/Laptop - Jaringan Internet - Bukti Insiden - Tiket Laporan	5 Menit	Formulir Laporan Insiden dan Tiket Laporan	
4	Petugas Melakukan Verifikasi kebenaran terkait insiden keamanan informasi yang disampaikan oleh Pelapor.		 Tidak Sesuai Sesuai			- PC/Laptop - Jaringan Internet - Media Komunikasi - Logbook Keamanan Siber	20 Menit	Laporan Insiden	Melakukan verifikasi kebenaran laporan insiden
5	Petugas Melakukan Kategorisasi Laporan terkait status dan prioritas Insiden Keamanan Informasi yang terjadi.					- PC/Laptop - Jaringan Internet - Media Komunikasi - Logbook Keamanan Siber	5 Menit	Kategorisasi Laporan Insiden	Mengkategorisasi Laporan Insiden sesuai dengan penanganannya
6	Petugas Menganalisa dan Mengevaluasi Laporan Insiden : a. Jika Insiden berkaitan dengan pelanggaran hukum perundang – undangan serta kebijakan yang berlaku, maka dibuatkan laporan lanjutan dan melakukan					- PC/Laptop - Jaringan Internet - Data Pelapor dan Laporan Insiden - Bukti Insiden - Media Komunikasi	1 Hari	Konfirmasi dan Rekomendasi Penanganan Insiden	

	koordinasi dengan Pihak yang Berwajib / Aparat Penegak Hukum (APH). b. Jika Insiden tidak berkaitan dengan pelanggaran hukum perundang – undangan serta kebijakan yang berlaku, maka petugas memberikan form laporan insiden tersebut ke Tim TTIS KUKARKAB.		A	B		C				
7	Pihak Berwajib / Aparat Penegak Hukum (APH) menerima Laporan yang disampaikan oleh Petugas dan melakukan Tindakan Penanganan Insiden Keamanan Informasi.						• PC/Laptop • Jaringan Internet • Data Pelapor dan Laporan Insiden • Bukti Insiden • Media Komunikasi	2 Hari	Konfirmasi dan Langkah Penanganan Insiden Keamanan Informasi terkait Hukum	
8	Pihak Berwajib / Aparat Penegak Hukum (APH) memberikan Laporan terkait hasil Penanganan Insiden Keamanan Informasi Kepada Petugas.						• PC/Laptop/Printer • Jaringan Internet • Media Komunikasi	1 Hari	Laporan Hasil Penanganan Insiden dari Pihak berwajib	
9	TTIS KUKARKAB melakukan Tindakan perbaikan insiden tersebut sesuai dengan laporan insiden.						• PC/Laptop • Jaringan Internet • Tools Keamanan Siber	1 Hari	Konfirmasi dan Langkah Perbaikan Insiden dari TTIS KUKARKAB	Menindaklanjuti perbaikan insiden sesuai laporan dari pihak berwajib
10	Petugas beserta TTIS KUKARKAB melakukan Analisa terhadap penyelesaian insiden yang dilaporkan.						• PC/Laptop • Jaringan Internet • Laporan Insiden • Tools Keamanan Siber	1 Hari	Laporan Hasil Penanganan Insiden dari TTIS KUKARKAB	
11	Petugas mengupdate Log Gangguan Keamanan Informasi.						• PC/Laptop • Jaringan Internet • Logbook Keamanan Siber	10 Menit	Up to Date Logbook Keamanan Siber	

12	Proses Pelaporan Insiden Keamanan Informasi dapat dinyatakan Selesai.				• PC/Laptop/Printer	1 Hari	Laporan Penanganan Insiden Siber	
----	---	--	---	--	---	--------	----------------------------------	--