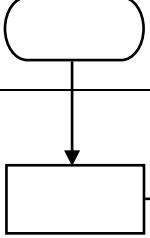
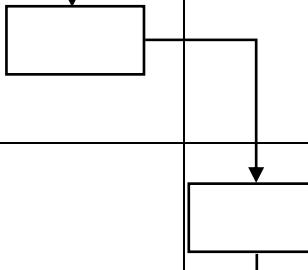
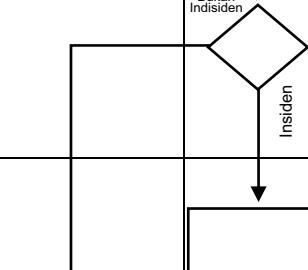
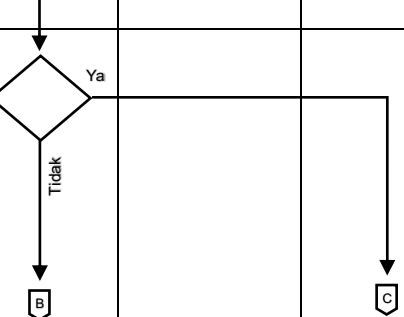


 <p>DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN TRENGGALEK</p>	Nama SOP	SOP Layanan Insiden Keamanan Informasi
	Nomor SOP	500.12.10/13/406.020/2025
	Tanggal Pembuatan	-
	Tanggal Revisi	-
	Tanggal Pengesahan	2 Desember 2025
	Disahkan Oleh	<p>Plt. Kepala Dinas Komunikasi dan Informatika Kabupaten Trenggalek</p>  <p>ARIEF SETIAWAN, SE, M.Si NIP. 19810507 201001 1 017</p>
DASAR HUKUM	KUALIFIKASI PELAKSANA	
<ol style="list-style-type: none"> Undang-undang Nomor 25 Tahun 2009 tentang Pelayanan Publik Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi RI No 35 Tahun 2012 tentang Pedoman Penyusunan SOP Adminstrasi Pemerintahan Peraturan Menteri Dalam Negeri No 52 tahun 2011 tentang SOP di Lingkungan Pemerintah Provinsi dan Kabupaten/Kota Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah 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 Peraturan Bupati (Perbup) Kabupaten Trenggalek Nomor 11 Tahun 2022 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah 	<ol style="list-style-type: none"> Kabid dan Kasi : <ul style="list-style-type: none"> Memiliki kemampuan interpersonal yang baik Technical Support : <ul style="list-style-type: none"> SDM yang memiliki kompetensi IT SDM yang memahami peraturan - peraturan dan kebijakan terkait Insiden Keamanan Informasi 	

KETERKAITAN	PERLENGKAPAN/PERSYARATAN
-	<ol style="list-style-type: none"> 1. Laporan Insiden 2. PC/Laptop/Printer; 3. Tools (Keamanan Siber) Perangkat Komputer; 4. Media Komunikasi;
PERINGATAN	PENCATATAN DAN PENDATAAN
Apabila SOP Layanan Insiden Keamanan Informasi tidakdijalankan dengan baik maka proses Penanganan Insiden Keamanan Informasi akan tidak berjalan efektif	<ol style="list-style-type: none"> 1. 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	Petugas	TTIS TrenggalekKab	Aparat Penegak Hukum	Kelengkapan	Waktu	Output	
1	Proses Laporan Dugaan Insiden Keamanan dimulai					Laporan Insiden	5 Menit	Laporan Insiden	
2	Menerima laporan adanya dugaan insiden siber, laporan dapat berasal dari pihak luar maupun dari Tim Internal Perangkat Daerah (PD).					<ul style="list-style-type: none"> • Data Pelapor dan Laporan Insiden • Bukti Insiden • Media Komunikasi 	10 Menit	Formulir Laporan Insiden	
3	Menginput Laporan Insiden terkait keamanan informasi berdasarkan informasi yang disampaikan oleh Pelapor.					<ul style="list-style-type: none"> • Bukti Insiden • Tiket Laporan 	10 Menit	Formulir Laporan Insiden dan Tiket Laporan	
4	Verifikasi kebenaran terkait insiden keamanan informasi yang disampaikan oleh Pelapor.					<ul style="list-style-type: none"> • Media Komunikasi • Logbook Keamanan Siber 	20 Menit	Laporan Insiden	Melakukan verifikasi kebenaran laporan insiden
5	Melakukan Kategorisasi Laporan terkait status dan prioritas Insiden Keamanan Informasi yang terjadi.					<ul style="list-style-type: none"> • Media Komunikasi • Logbook Keamanan Siber 	10 Menit	Kategorisasi Laporan Insiden	Mengkategorisasi Laporan Insiden sesuai dengan penanganannya
6	Menganalisa dan Mengevaluasi Laporan Insiden : a. Ya, Jika Insiden berkaitan dengan pelanggaran hukum, perundang–undangan serta kebijakan yang berlaku, maka dibuatkan laporan lanjutan dan melakukan					<ul style="list-style-type: none"> • Laptop • Data Pelapor dan Laporan Insiden • Bukti Insiden • Media Komunikasi 	1 Hari	Konfirmasi dan Rekomendasi Penanganan Insiden	

	<p>koordinasi dengan <i>Aparat Penegak Hukum (APH)</i>.</p> <p>b. Tidak, Jika Insiden tidak berkaitan dengan pelanggaran hukum, perundang – undangan serta kebijakan yang berlaku, maka petugas memberikan laporan insiden tersebut ke <i>Tim TTIS Trenggalek</i>.</p>	A	B		C			
7	Aparat Penegak Hukum (APH) menerima Laporan yang disampaikan oleh Petugas dan melakukan Tindakan Penanganan Insiden Keamanan Informasi.					<ul style="list-style-type: none"> • Data Pelapor dan Laporan Insiden • Bukti Insiden • Media Komunikasi 	2 Hari	Konfirmasi dan Langkah Penanganan Insiden Keamanan Informasi terkait Hukum
8	Aparat Penegak Hukum (APH) memberikan Laporan terkait hasil Penanganan Insiden Keamanan Informasi					<ul style="list-style-type: none"> • Data Pelapor dan Laporan Insiden • Bukti Insiden • Media Komunikasi 	1 Hari	Laporan Hasil Penanganan Insiden dari Aparat Penegak Hukum
9	Melakukan perbaikan insiden tersebut sesuai dengan laporan insiden.					<ul style="list-style-type: none"> • Tools Keamanan Siber 	1 Hari	Konfirmasi dan Langkah Perbaikan Insiden dari TTIS Trenggalek
10	Melakukan Analisa terhadap penyelesaian insiden yang dilaporkan.					<ul style="list-style-type: none"> • Laporan Insiden • Tools Keamanan Siber 	1 Hari	Laporan Hasil Penanganan Insiden dari TTIS Trenggalek
11	Update Hasil Penanganan Insiden Keamanan Informasi.					<ul style="list-style-type: none"> • Logbook Keamanan Siber 	10 Menit	Up to Date Logbook Keamanan Siber
12	Pelaporan Insiden Keamanan Informasi dapat dinyatakan Selesai.					<ul style="list-style-type: none"> • Laporan 	1 Hari	Laporan Penanganan Insiden Siber