DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN TAPIN

Nomor SOP	000.8.3.3/011.g/DISKOMINFO/I/2024
Tanggal Pembuatan	14 Agustus 2023
Tanggal Revisi	8 Januari 2024
Tanggal Efektif	
Disahkan Oleh	Kepala Dinas Komunikasi dan Informatika Kabupaten Tapin **Wahyudi Pranoto, S.Sos, MT** **Pembina Tk I/ IV/b** NIP 19710130 199903 1 005
Nama SOP	Penanganan Insiden Siber

Dasar Hukum :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
2. Undang-Undang Nomor 72 Tahun 2022 tentang Infrastruktur Informasi Vital
3. Peraturan Presiden No.95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) Pasal 40 dan 41 (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182).
4. Peraturan Kepala BSSN No. 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik
5. Peraturan Kepala BSSN No. 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis ELektronik
6. Peraturan Bupati Tapin No. 16 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik

Keterkaitan :

Peringatan :

Dan jika SOP ini tidak dilaksanakan akan mengakibatkan tidak tertanganinya insiden siber secara efektif, efisien, dan tidak dapat dipertanggung jawabkan.

Kualifikasi Pelaksana :

1. TIM Penanggulangan dan Pemulihan Insiden adalah Tim Keamanan Informasi yang harus memiliki kemampuan analisia risiko dan memiliki kemampuan komunikasi dan koordinasi yang baik.
2. Sub Tim Koordinasi Insiden adalah Tim yang bertugas untuk menerima, mendokumentasikan, meneruskan laporan insiden, melakukan triase insiden dan menginformasikan status insiden.
3. Sub Tim Keamanan Informasi adalah Tim yang bertugas untuk melakukan deteksi, identifikasi, analisis terhadapa celah keamanan, analisis resiko, memberikan petunjuk dan arahan untuk menanggulangi insiden siber.
4. Sub Tim Jaringan dan Server adalah Tim yang bertugas untuk melakukan pemantauan, pengelolaan terhadap lalu lintas data pada jaringan dan kinerja server.
5. Sub Tim Website dan Aplikasi adalah Tim yang bertugas untuk melakukan pemantauan, pengelolaan terhadap website dan aplikasi.
6. Sub Tim Pengelola Data Insiden adalah Tim yang bertugas untuk helpdesk/pusat pelaporan.
7. Koordinator SKPD bertugas sebagai narahubung antara Tim Keamanan Informasi, Tim Server dan Jaringan, Tim Website dan Aplikasi, Tim Koordinasi Insiden dan Tim Pengelola Data Insiden.

Peralatan / Perlengkapan :

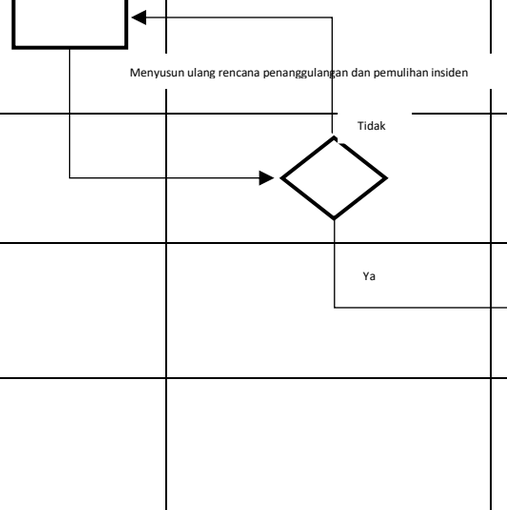
1. Perangkat Komputer
2. Perangkat Deteksi dan Analisa Keamanan Siber
3. Perangkat Monitoring Jaringan
4. Perangkat Monitoring Aplikasi dan Website
5. Perangkat Pencetak Dokumen

Pencatatan dan Pendataan :

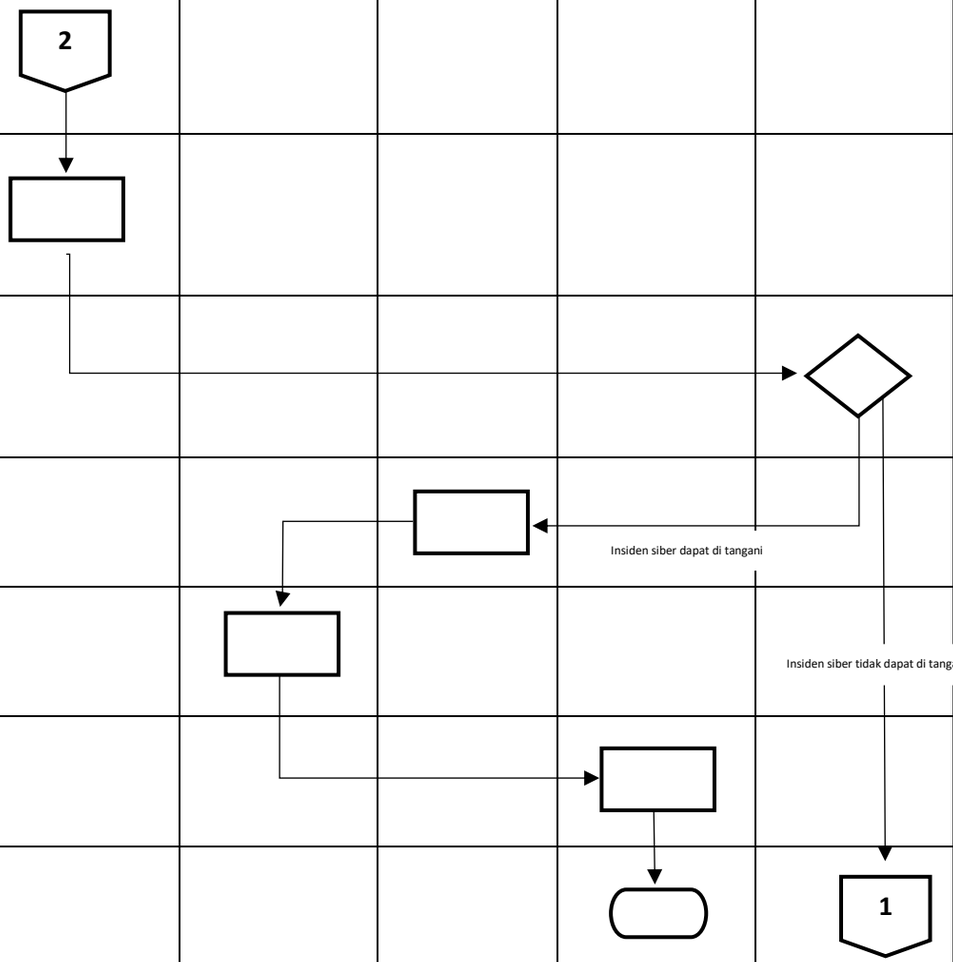
1. Laporan Hasil Penanganan Insiden Siber

No	Aktivitas	Pelaksana							Mutu Baku			Ket
		Pelapor	Sub Tim Pengelola Data Insiden	Sub Tim Koordinasi Insiden	Sub Tim Keamanan Informasi	Koordinator SKPD / POC			Persyaratan dan Kelengkapan	Waktu	Output	
1	Melaporkan gangguan akibat anomali/gangguan yang sedang terjadi dalam sistem								Laporan	20 Menit	Laporan	
2	Menerima laporan gangguan dari pelapor internal Diskominfo dan Eksternal								Laporan	20 Menit	Laporan	
3	Menerima, mendokumentasikan, melakukan triase insiden dan meneruskan laporan insiden dari informasi koordinator SKPD								Dokumen	80 Menit	Dokumen	
4	Melaporkan insiden siber yang terjadi pada sistem elektronik								Laporan	30 Menit	Laporan	
5	Menerima laporan insiden siber dari Koordinator SKPD				1				Laporan	20 Menit	Laporan	

No	Aktivitas	Pelaksana							Mutu Baku			Ket
		Sub Tim Keamanan Informasi	Koordinator Tim Penanggulangan dan Pemulihan Insiden	Koordinator SKPD / POC	Sub Tim Website dan Aplikasi	Sub Tim Jaringan dan Server			Persyaratan dan Kelengkapan	Waktu	Output	
1	Menerima laporan insiden siber dari Koordinator SKPD	1							Laporan	20 Menit	Laporan	
2	Melakukan deteksi, identifikasi, analisis terhadap celah keamanan informasi dan menyusun rencana penanggulangan dan pemulihan insiden								Dokumen	80 Menit	Dokumen	
3	Memberikan persetujuan untuk melakukan tindakan								Surat	20 Menit	Surat	
4	Melaporkan insiden siber yang terjadi hasil dari analisis tim keamanan informasi								Laporan	30 Menit	Laporan	
5	Menerima laporan hasil dari analisis dan melakukan tindakan pemulihan				2	3			Laporan	20 Menit	Laporan	



No	Aktivitas	Pelaksana							Mutu Baku			Ket
		Sub Tim Website dan Aplikasi	Sub Tim Pengelola Data Insiden	Sub Tim Koordinasi Insiden	Pelapor	Koordinator SKPD / POC			Persyaratan dan Kelengkapan	Waktu	Output	
1	Menerima laporan hasil dari analisis dan melakukan tindakan pemulihan								Laporan	20 Menit	Laporan	
2	Melaksanakan Penanggulangan dan Pemulihan Insiden								Laporan	80 Menit	Laporan	
3	Menyusun dan menyampaikan laporan hasil tindak lanjut Sub Tim Website dan Aplikasi								Laporan	30 Menit	Laporan	
4	Menerima, mencatat dan menginformasikan status insiden siber yang dilaporkan								Laporan	60 Menit	Laporan	
5	Menerima dan menginformasi hasil tindak lanjut insiden siber								Laporan	30 Menit	Laporan	
6	Menerima informasi status insiden siber								Laporan	20 Menit	Laporan	
7	Selesai											



No	Aktivitas	Pelaksana							Mutu Baku			Ket
		Sub Tim Jaringan dan Server	Sub Tim Pengelola Data Insiden	Sub Tim Koordinasi Insiden	Pelapor	Koordinator SKPD / POC			Persyaratan dan Kelengkapan	Waktu	Output	
1	Menerima laporan hasil dari analisis dan melakukan tindakan pemulihan								Laporan	20 Menit	Laporan	
2	Melaksanakan Penanggulangan dan Pemulihan Insiden								Laporan	80 Menit	Laporan	
3	Menyusun dan menyampaikan laporan hasil tindak lanjut Sub Tim Website dan Aplikasi								Laporan	30 Menit	Laporan	
4	Menerima, mencatat dan menginformasikan status insiden siber yang dilaporkan								Laporan	60 Menit	Laporan	
5	Menerima dan menginformasi hasil tindak lanjut insiden siber								Laporan	30 Menit	Laporan	
6	Menerima informasi status insiden siber								Laporan	20 Menit	Laporan	
7	Selesai