










Nomor SOP			DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN TEGAL
Tanggal Pembuatan			
Tanggal Revisi			
Tanggal Pengesahan			
Disahkan oleh	 Dra NURHAYATI, MM NIP. 197004261990012001		
Nama SOP	SOP Pelaporan dan Penanganan Insiden Siber		

Dasar Hukum	Kualifikasi Pelaksana
<ol style="list-style-type: none"> Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBF dan Standar Teknis dan Prosedur Keamanan SPBF Peraturan Daerah Kabupaten Tegal Nomor 2 Tahun 2020 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Kabupaten Tegal Peraturan Daerah Kabupaten Tegal Nomor 10 Tahun 2021 tentang Perubahan Kedua Atas Peraturan Daerah Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Tegal Peraturan Bupati Tegal Nomor 82 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Perangkat Daerah dan Staf Ahli Bupati di Lingkungan Pemerintah Kabupaten Tegal 	<ol style="list-style-type: none"> Memiliki kemampuan mengoperasikan server Memiliki kemampuan mengoperasikan tools penanggulangan dan atau pemulihan insiden keamanan siber Memiliki kemampuan membaca log server Memiliki kemampuan membaca topologi jaringan Memiliki kemampuan analisis penyebab terjadinya insiden siber

Keterkaitan	Peralatan / Perlengkapan
<ol style="list-style-type: none"> SOP Pelayanan Administrasi Surat Masuk SOP Pelayanan Administrasi Surat Keluar 	<ol style="list-style-type: none"> Komputer dan atau Laptop Server Tools penanggulangan dan pemulihan sistem
Peringatan	Pencatatan dan Pendataan
<ol style="list-style-type: none"> Apabila prosedur ini dilaksanakan, aplikasi yang berjalan di server dapat terpantau dan ditindaklanjuti secara cepat ketika terjadi insiden maupun serangan siber Apabila prosedur ini tidak dapat dilaksanakan, aplikasi yang menjadi sasaran insiden maupun serangan siber tidak dapat dilakukan upaya penanganan dan dapat menjadi celah keamanan yang mengancam aplikasi-aplikasi lainnya yang berada dalam satu server dengan aplikasi tersebut Apabila prosedur ini dilaksanakan oleh pihak-pihak atau individu yang kurang atau tidak memiliki kompetensi yang disebutkan, maka proses pelaporan dan penanganan insiden siber tidak akan berjalan dengan baik karena aspek-aspek yang harus dilaporkan, dianalisis, diperbaiki, dan diperbaharui tidak teridentifikasi secara lengkap 	<ol style="list-style-type: none"> Laporan insiden siber dapat berasal dari pihak internal perangkat daerah, pemilik aplikasi, pihak luar baik yang mewakili instansi maupun perorangan Laporan Analisis Penyebab Insiden Siber Rekomendasi Penanggulangan Insiden Siber
Pelaksana	
<ol style="list-style-type: none"> Dinas Komunikasi dan Informatika Kab. Tegal Tim Penanganan Insiden Siber JatengProv-CSIRT atau Badan Siber dan Sandi Negara Organisasi Perangkat Daerah Pemilik atau Penanggung Jawa Aplikasi Pengembang Aplikasi (Pihak Ketiga maupun Tim Internal OPD) 	

No	Uraian Kegiatan	Pelaksana					Mutu Baku			Ket
		1	2	3	4	5	Perlengkapan	Waktu	Output	
1.	Menerima laporan insiden siber (laporan dapat berasal dari internal dan pihak luar)						<ul style="list-style-type: none"> • Komputer • Laptop • Email 	10 menit	Laporan insiden siber	
2.	Mencruskan laporan insiden kepada TegalKab-CSIRT						<ul style="list-style-type: none"> • Laporan Insiden Siber • Komputer • Laptop • Email 	10 menit	Laporan insiden siber diterima TegalKab-CSIRT	
3.	Melakukan verifikasi atas laporan insiden siber terkait: <ul style="list-style-type: none"> • Jenis Insiden Siber • Identitas Pelapor • Sistem Log Hasil verifikasi berupa: <ul style="list-style-type: none"> • Laporan Valid, untuk segera ditindaklanjuti • Laporan tida Valid 	Tidak Valid				<ul style="list-style-type: none"> • Laporan Insiden Siber • Komputer • Laptop • Email • Server • E-Ticketing 	30 menit	Laporan terverifikasi		
4.	Menyusun strategi mitigasi terhadap insiden siber, antara lain: <ul style="list-style-type: none"> • Suspend domain • Backup data • Melokalisir aplikasi • Menutup port tertentu • Strategi-strategi lainnya terkait penanganan dan penanggulangan insiden 					Laporan Insiden Siber	30 menit	Langkah penanganan sementara insiden siber		
5.	Melaksanakan penanganan insiden siber sesuai strategi yang disusun					<ul style="list-style-type: none"> • Laporan Insiden Siber • Komputer • Laptop • Server 	10-30 menit			
6.	Melakukan analisis lanjutan atas insiden siber yang terjadi					<ul style="list-style-type: none"> • Laporan Insiden Siber • Komputer • Laptop • Server 	1-3 hari	Laporan Analisis Insiden Siber dan Rekomendasi Penanganan Insiden Siber		
7.	Menyampaikan laporan insiden siber, laporan analisis dan rekomendasi solusi insiden siber ke JatengProv CSIRT atau BSSN, OPD yang terdampak dan tembusan kepada Sekretaris Daerah sebagai laporan					Laporan Analisis Insiden Siber dan Rekomendasi Penanganan Insiden Siber				
8.	Menindaklanjuti laporan dalam bentuk rekomendasi dan eskalasi ke JatengProv CSIRT atau BSSN					Laporan Analisis Insiden Siber dan Rekomendasi Penanganan Insiden Siber				

9.	Menindaklanjuti laporan dan rekomendasi dari JatengProv CSIRT atau BSSN dan atau berkoordinasi dengan pihak pengembang aplikasi					Laporan Analisis Insiden Siber dan Rekomendasi Penanganan Insiden Siber			
10.	Memberikan tanggapan berupa langkah-langkah penanganan insiden yang telah dilaksanakan sesuai rekomendasi					<ul style="list-style-type: none"> • Komputer • Laptop • Email 			
11.	Menyusun Laporan Pcnanganan Insiden Siber					<ul style="list-style-type: none"> • Komputer • Laptop • Printer 			