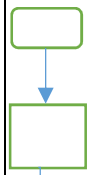
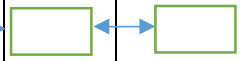
Nomor SOP			DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK KOTA DENPASAR
Tanggal Pembuatan			
Tanggal Revisi			
Tanggal Pengesahan			
Disahkan Oleh	Kepala Dinas Komunikasi Informatika Dan Statistik Kota Denpasar Dr.IDA BAGUS ALIT ADHI MERTA,SSTP,M.Si Nip.197801281996121003		
Nama SOP	SOP Laporan dan Penanganan Insident Siber		

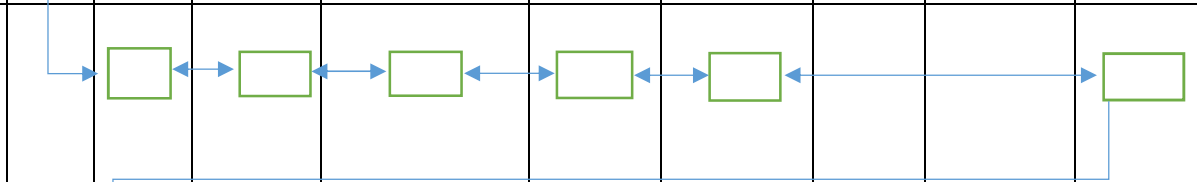
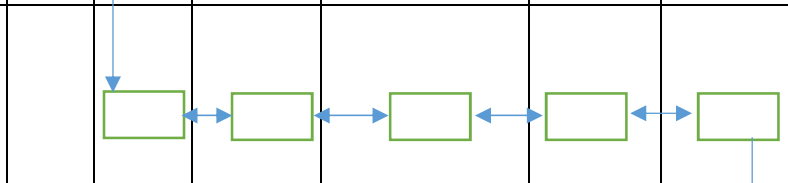
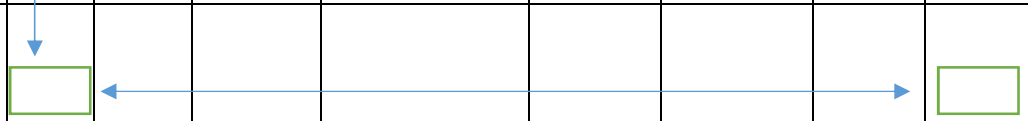
Dasar Hukum	Kualifikasi Pelaksana
1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik 2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 Tentang Pelaksanaan Persandian untuk Pengamanan informasi di Pemerintahan Daerah 3. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Kemanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541) 4. Keputusan Walikota Denpasar Nomor 188,45/1272/Hk/2022 tentang pembentukan Computer Security Incident Response Team Kota Denpasar (Denpasar CSIRT)	1. Memiliki kemampuan mengoperasikan server 2. Memiliki kemampuan mengoperasikan tools penanggulangan pemulihan insiden keamanan siber 3. Memiliki kemampuan membaca topologi jaringan 4. Memiliki kemampuan membaca log server 5. Memiliki kemampuan analisis penyebab insiden siber

Keterkaitan	Peralatan/Perlengkapan
1. SOP Pelayanan Administrasi Surat Masuk 2. SOP Pelayanan Administrasi Surat Keluar	1. Komputer 2. Server 3. Tools penanggulangan insiden dan pemulihan sistem
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. Apabila prosedur ini tidak dilaksanakan,Aplikasi menjadi sasaran insiden maupun serangan siber tidak dapat segera diperbaiki dan bisa menjadi celah keamanan yang mengancam aplikasi-aplikasi lain yang berada dalam satu server dengan aplikasi tersebut.	1. Laporan insiden siber, berasal dari internal PD diskominfo maupun pemilik aplikasi serta pihak luar, baik yang mewakili instansi maupun perseorangan mengenai celah keamanan, tidak dapat diaksesnya suatu aplikasi, maupun hal lain yang termasuk dalam kategori insiden siber. 2. Laporan Analisis Penyebab Insiden Siber serta rekomendasi Penanggulangan Insiden Siber

3. Apabila 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.	
Pelaksana	
1. Dinas Komunikasi, Informatika dan Statistik Kota Denpasar 2. Tim Denpasar-CSIRT (pengelola jaringan dan server, keamanan informasi, website administrator dan aplikasi) 3. Tim Bali Prov-CSIRT atau Badan Siber dan Sandi Negara (BSSN) 4. Perangkat Daerah Penanggung Jawab Aplikasi 5. Pengembang Aplikasi (Pihak ketiga maupun Tim Interal bentukan PD)	

NO	Uraian Kegiatan	Pelaksana								Mutu Baku			Ket.
		1 DKIS	2 TIM DENPASAR-CSIRT					3 BALI PROV-CSIRT/ BSSN	4 PERANGKAT DAERAH	5 PENGEMBANG	Perlengkapan	Waktu	Output	
			SERVER	JARINGAN	WEBSITE ADMINISTRATOR	APLIKASI	KEAMANAN INFORMASI							
1	Menerima laporan insiden siber, laporan dapat berasal dari pihak luar maupun dari tim internal PD (surat/email)										- Komputer - Email - Surat	5 Menit	- Laporan Insiden Siber	
2	Meneruskan laporan insiden kepada Tim Denpasar-CSIRT										- Laporan Insiden Siber - Komputer - Email - Surat	10 Menit	- Laporan Insiden Siber diterima Tim Denpasar -CSIRT	

3	Tim Denpasar-CSIRT Melakukan verifikasi atas laporan insiden siber terkait: - Identitas Pelapor - Jenis Insiden Siber - Lokasi server - Sistem log Hasil Verifikasi berupa: a. Laporan Valid, Untuk segera ditindak lanjuti b. Laporan tidak Valid										- Laporan Insiden Siber - Komputer - Server - Aplikasi/Web site - Tool Web devicement	2 hari	- Laporan verifikasi	- Laporan valid (terkait serangan siber) - Laporan tidak valid (tidak ada indikasi serangan siber)
4	Menyusun Strategi mitigasi terhadap insiden siber (Non aktif Domain ,mengganti tampilan dengan undercontruction/maintanance, Backup data)										- Komputer - Server - Aplikasi/Web site	1 hari	- Langkah Penanganan sementara insiden siber (Non aktif Domain ,mengganti tampilan dengan undercontruction/maintanance, Backup data)	
5	Melaksanakan penanganan insiden siber sesuai strategi mitigasi yang di susun										- Komputer - Server - Aplikasi/Web site - Tools - Laporan analisis penangan insiden siber	3 hari	- Laporan penanganan insiden siber - Laporan penanganan insiden siber yang belum berhasil di tangani	- jika tidak bisa ditangani dilanjutkan berkoordinasi dengan Vendor/Bali Prov-CSIRT/BSSN
6	Menyampaikan laporan analisis dan rekomendasi inseden siber ke Bali Prov-CSIRT dan BSSN serta PD terkait tembusan kepada Sekretaris Daerah sebagai laporan										- Laporan Analisis Insiden Siber dan rekomendasi penanganan inseden siber - Email -	1 hari	- Laporan rekomendasi dari Bali Prov-CSIRT/BSSN/PD terkait	-

7	Menindak lanjuti laporan (dalam bentuk rekomendasi) dan eskalasi ke BSSN apabila di perlukan										- Laporan Analisis Insiden Siber dan Rekomendasi Penanganan Insiden siber - Komputer - Server - Aplikasi/Website - Tools	1 hari	- Konfirmasi dan Rekomendasi Penanganan Siber	- Tools
8	Menindaklanjuti laporan (rekomendasi tim Denpasar CSIRT dan BSSN) dengan berkoordinasi dengan pihak pengembang aplikasi										- Laporan Rekomendasi Tim Denpasar-CSIRT dan BSSN - Email	30 menit	- Laporan rekomendasi hasil kordinasi	-
9	Memberikan tanggapan berupa langkah-langkah penanganan insiden yang telah dilaksanakan berdasarkan rekomendasi										- Komputer - Email - Server - Aplikasi/Website -	1 hari	- Tanggapan Laporan Siber	-
10	Menyusun Laporan Penanganan Insiden Siber										- Komputer	3 hari	- Laporan Penanganan Insiden Siber	-