PEMERINTAH KOTA BATAM

BIDANG PENGELOLAAN INFORMASI PUBLIK DAN PERSANDIAN
DINAS KOMUNIKASI DAN INFORMATIKA

STANDAR OPERASIONAL PROSEDUR (SOP)

LAPORAN DAN PENANGANAN INSIDEN SIBER

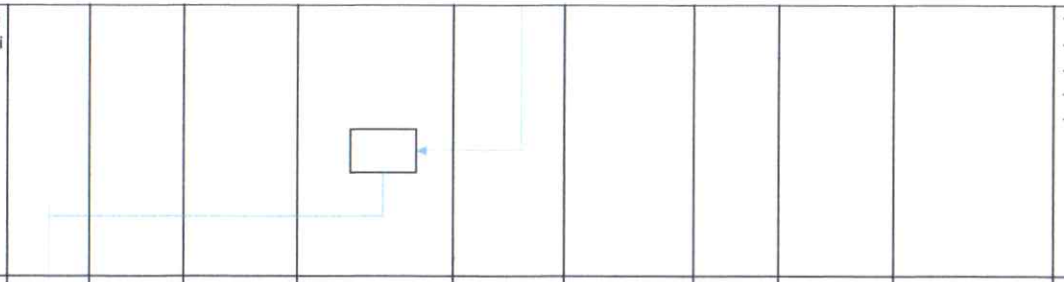
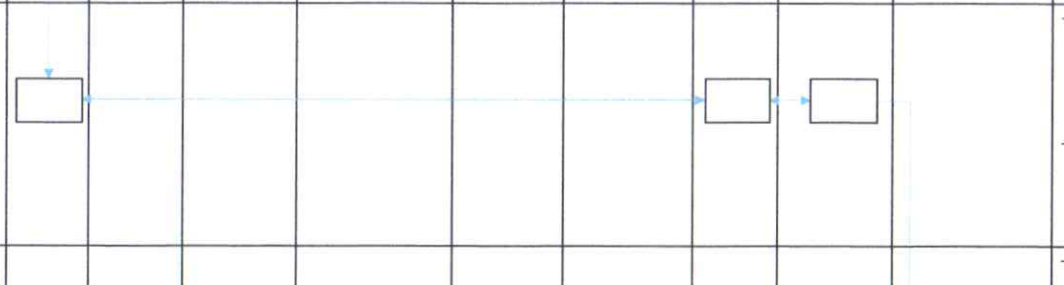
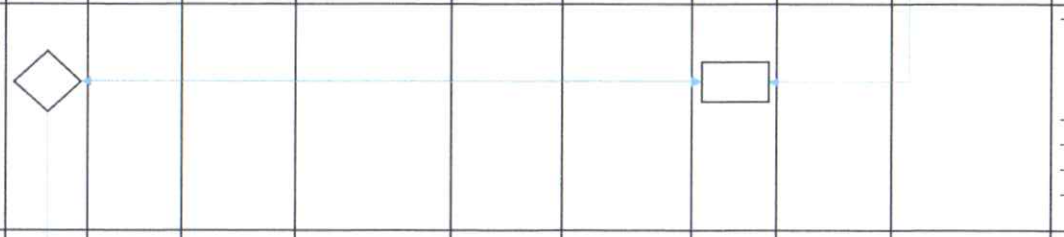
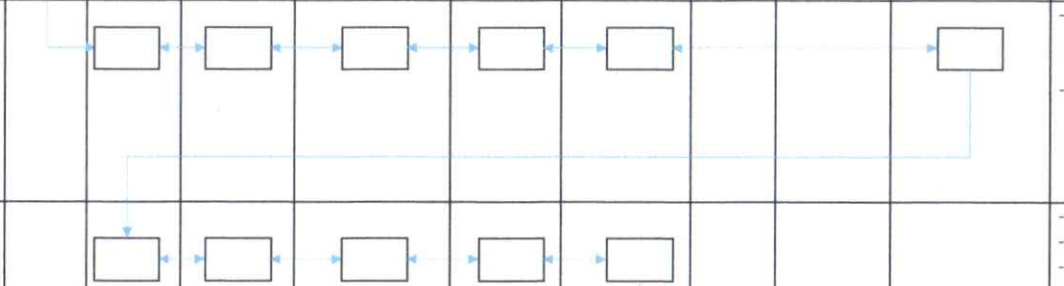
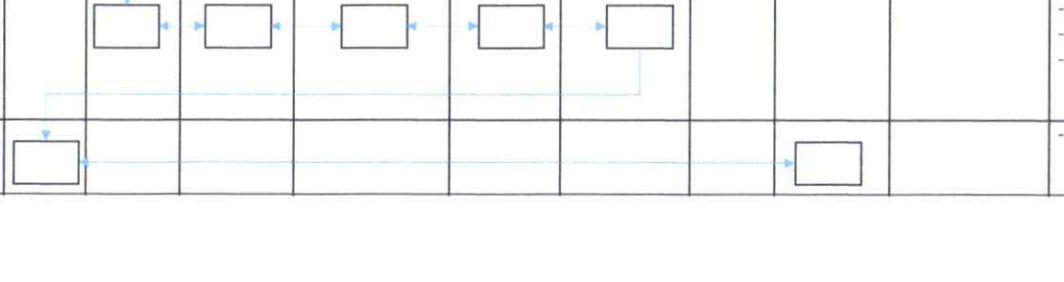
PEMERINTAH KOTA BATAM
DINAS KOMUNIKASI DAN INFORMATIKA

BIDANG PENGELOLAAN INFORMASI PUBLIK DAN PERSANDIAN

Nomor SOP	01/SOP/Kominfo-PIPP/VIII/2023
Tanggal Pembuatan	31 Agustus 2023
Tanggal Revisi	-
Tanggal Pengesahan	31 Agustus 2023
Disahkan oleh	Kepala Dinas Komunikasi dan Informatika Kota Batam **Rudi Panjaitan, S.STP., M.Si** Pembina Tingkat I NIP. 19761123 199511 1 002
Judul SOP	**Laporan dan Penanganan Insiden 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 NegaraNomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541) 4. Peraturan Wali Kota Batam Nomor 65 Tahun 2022 tentang Penyelenggaran Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kota Batam 5. Keputusan Wali Kota Batam Nomor 393 Tahun 2022 tentang Tim Tanggal Insiden Siber Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kota Batam	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 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	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

No	Uraian Kegiatan	Pelaksana								Mutu Baku			Ket
		1 Diskominfo	2 TIM BATAM-CSIRT				3 KEPRI PROV-CSIRT/BSSN	4 PERANGKAT DAERAH	5 PENGEMBANGAN	Perlengkapan	Waktu	Output	
			KETUA	SEKRETARIS	KOORDINATOR	TIM BATAM- CSIRT							
1	Menerima laporan insiden siber, laporan dapat berasal dari pihak luar maupuan dari tim internal PD (surat/email)									- Komputer - Email - Surat	5 menit	- Laporan Insiden Siber	
2	Meneruskan laporan insiden kepada Tim BATAM-CSIRT									- Laporan Insiden Siber - Komputer - Email - Surat	10 menit	- Laporan Insiden Siber diterima Tim BATAM -CSIRT	
3	Tim BATAM-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/Website - 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 Domai, mengganti tampilan dengan undercontruction/maintenance, Backup data)									- Komputer - Server - Aplikasi/Website	1 hari	- Langkah penanganan sementara insiden siber (Non aktif Domain, mengganti tampilan dengan undercontruction/ maintance Backup data)	

5	Melaksanakan penanganan insiden siber sesuai strategi mitigasi yang disusun									- Komputer - Server - Aplikasi/Website - 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 dengan berkoordinasi dengan Vendor/KEPRIPROV-CSIRT/BSSN
6	Menyampaikan laporan analisis dan rekomendasi insiden siber KEPRIPROV-CSIRT dan BSSN serta Perangkat Daerah (PD) terkait tembusan kepada Sekretaris Daerah sebagai laporan									- Laporan Analisis Insiden Siber dan Rekomendasi Penanganan Insiden Siber Email -	1 hari	- Laporan rekomendasi dari KEPRIPROV-CSIRT/BSSN/PD terkait	
7	Menindaklanjuti 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 BATAM-CSIRT dan BSSN) dengan berkoordinasi dengan pihak pengembangan aplikasi									- Laporan Rekomendasi Tim BATAM-CSIRT dan BSSN Email -	30 menit	- Laporan rekomendasi hasil koordinasi	
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	