STANDART OPERASIONAL PROSEDUR
LAPORAN DAN PENANGANAN INSIDEN SIBER

2025

DINAS KOMUNIKASI, INFORMATIKA DAN PERSANDIAN
PROVINSI MALUKU UTARA

Alamat : Jalan Trans Halmahera Gosale Puncak
S O F I F I

CATATAN :

1 *Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertfikat Elektronik (BSrE), Badan Siber dan Sandi Negara;*
2 *Dokumen ini dapat di validasi melalui aplikasi Besign Desktop, Besign dan Adobe Reader;*
3 *Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah sesuai dengan UU ITE No 11 Tahun 2008 Pasal 5 Ayat.*

DINAS KOMUNIKASI, INFORMATRTIKA DAN STATISTIK PROVINSI MALUKU UTARA **BIDANG PERSANDIAN DAN STATISTIK**	Nomor SOP	:	000.6 / 231 / DKIP-MU / VIII / 2025
	Tanggal Pembuatan	:	14 Agustus 2025
	Tanggal Revisi	:	-
	Tanggal Efektif	:	14 Agustus 2025
	Disahkan oleh	:	Ditandatangani secara elektronik oleh : KEPALA DINAS KOMUNIKASI, INFORMATIKA DAN PERSANDIAN PROVINSI MALUKU UTARA **Dr. IKSAN R.A. ARSAD, M.Si** Pembina Utama Madya
	Judul SOP	:	LAPORAN DAN PENANGANAN INSIDEN SIBER

Dasar Hukum	Kualifikasi Pelaksana
- Undang Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; - Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik - Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara; - Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE); - Peraturan Gubernur Maluku Utara Nomor : 27 Tahun 2019 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi dan Kabupaten_Kota - Keputusan Gubernur Maluku Utara nomor: 339/kpts/mu/2023 tentang tim tanggap insident siber (Computer Security Incident Response Team) /CSIRT Provinsi Maluku Utara	1. Memili kemampuan mengoperasikan server; 2. Memiliki kemampuan mengoperasikan tools penanggulangan pemulihan insiden keamanan siber; 3. Memiliki kemampuan membaca topologi jaringan; 4. Memiliki kkemampuan membaca log server; 5. Memiliki kemampuan analisis penyebab insiden siber; 6. Memili kemampuan koordinasi dengan pihak terkait; 7. Memiliki kemampuan mengoperasionalkan system tiketing; 8. Memiliki kemampuan melakukan pengamanan siber

CATATAN :

1 Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertfikat Elektronik (BSrE), Badan Siber dan Sandi Negara;
2 Dokumen ini dapat di validasi melalui aplikasi Besign Desktop, Besign dan Adobe Reader;
3 Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah sesuai dengan UU ITE No 11 Tahun 2008 Pasal 5 Ayat.

Keterkaitan SOP	Peralatan / Perlengkapan
- SOP COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) - SOP Pengaduan Insiden Keamanan Informasi (MaLut-CSIRT) - SOP ITSA (Information Technology Security Assesment) - SOP MANAJEMEN RISIKO	1. Komputer / Laptop 2. Server 3. Tools penanggulangan insiden dan pemulihan sistem 4. Jaringan Internet 5. Printer 6. Sistem ticket
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. Apa bila prosedur ini tidak dilaksanakan, aplikasi menjadi sasaran insiden maupun serangan siber tidak dapat segera di perbaiki dan bias menjasi celah keamanan yang mengancam aplikasi-aplikasi lain yang berada dalam satu server dengan aplikasi tersebut. 3. Apa bila 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 dilaporakan, dianalisis, diperabaiki, dan diperbahrui tidak terindefikasi secara lengkap.	1. Laporan insiden siber; berasal dari internal PD Diskominfosan maupun pemilik aplikasi serta pihak luar, baik yang mewakili instansi maupun perseorangan mengenai celah keamanan, tidak dapat di aksesnya suatu aplikasi, maupun hal lain yang termasuk dalam katagori insiden siber. 2. Laporan analis penyebab insiden siber serta rekomendasi penanggulangan insiden siber.

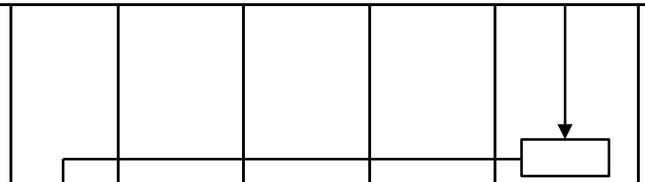
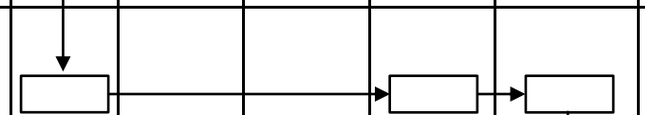
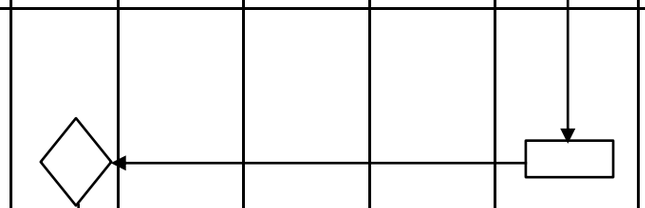
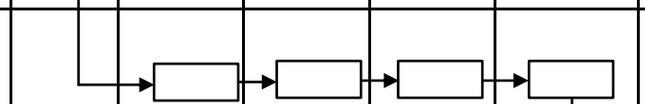
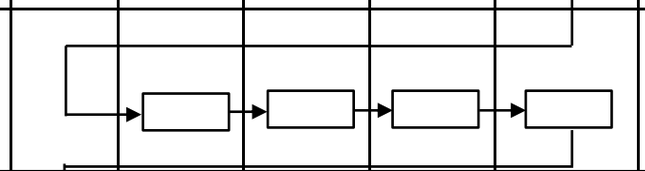
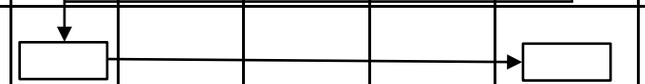
CATATAN :

1 Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertfikat Elektronik (BSrE), Badan Siber dan Sandi Negara;
2 Dokumen ini dapat di validasi melalui aplikasi Besign Desktop, Besign dan Adobe Reader;
3 Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah sesuai dengan UU ITE No 11 Tahun 2008 Pasal 5 Ayat.

No	KEGIATAN	PELAKSANA					MUTU BAKU			KET
		DISKOMINFOSAN	KETUA	SEKRETARIS	KOORDINATOR	TIM MALUT PROV-CSIRT DAN PENGEMBANG	PERLENGKAPAN	WAKTU	OUTPUT	
1	Menerima laporan insiden siber, laporan dapat berasal dari pihak luar maupun dari tim internal PD (surat/e-Mail)						- Komputer - e – Mail - Surat	5 Menit	Formulir aduan Insiden Siber	
2	Meneruskan aduan insiden keapada Tim Malutprov-CSIRT						- Laporan Insiden Siber - Komputer - e – Mail - Surat	10 Menit	Formulir aduan Insiden Siber diterima Tim Malutprov-CSIRT	
3	Tim Malutprov-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 ditindaklanjuti b. Laporan tidak valid						- Laporan Insiden Siber - Komputer - Server - Aplikasi/Website - Tool Web devicement	2 Hari	Formulir aduan Insiden Siber	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 / maintenance, Backup Data)						- Komputer - Server - Aplikasi/Website	1 Hari	Langkah penanganan sementara insiden siber (Non aktif Domain, mangganti tampilan dengan undercontruction/maintenance Backup data)	

CATATAN :

1 *Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertfikat Elektronik (BSrE), Badan Siber dan Sandi Negara;*
2 *Dokumen ini dapat di validasi melalui aplikasi Besign Desktop, Besign dan Adobe Reader;*
3 *Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah sesuai dengan UU ITE No 11 Tahun 2008 Pasal 5 Ayat.*

5	Mengidentifikasi insiden siber sesuai strategi mitigasi yang disusun		- Komputer - Server - Aplikasi/Website - Tools - Laporan analisis penanganan insiden siber	3 Hari	- Formulir Penanganan Insiden Siber - Laporan Penanganan Insiden Siber yang belum berhasil di tangani	Jika tidak bisa ditangani dilanjutkan dengan berkoordinasi dengan Pengembang/ BSSN
6	Menyampaikan hasil analisis dan rekomendasi insiden siber Tim Malutprov-CSIRT dan BSSN serta Perangkat Daerah (PD) terkait tembusan kepada Sekretariat Daerah sebagai laporan		Laporan Analis Insiden Siber dan Rekomendasi Penanganan Insiden Siber E-Mail	1 Hari	Laporan Rekomendasi dari Malutprov-CSIRT/BSSN/PD terkait	
7	Menindaklanjuti laporan (dalam bentuk rekomendasi) dan eskalasi ke BSSN apabila diperlukan		- 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 Malutprov-CSIRT dan BSSN) dengan berkoordinasi dengan pihak pengembang aplikasi		Laporan Rekomendasi Tim Malutprov-CSIRT dan BSSN e-Mail	30 Menit	Laporan hasil penanganan insiden	
9	Memberikan tanggapan berupa langkah – langkah penanganan insiden yang telah dilaksanakan berdasarkan rekomendasi		- Komputer - E-Mail - Server - Aplikasi/Website	1 Hari	Tanggapan Laporan Siber	
10	Menyusun Laporan Penanganan Insiden Siber		Komputer	3 Hari	Laporan Penanganan Insiden Siber	

CATATAN :

1 *Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertfikat Elektronik (BSrE), Badan Siber dan Sandi Negara;*
2 *Dokumen ini dapat di validasi melalui aplikasi Besign Desktop, Besign dan Adobe Reader;*
3 *Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah sesuai dengan UU ITE No 11 Tahun 2008 Pasal 5 Ayat.*