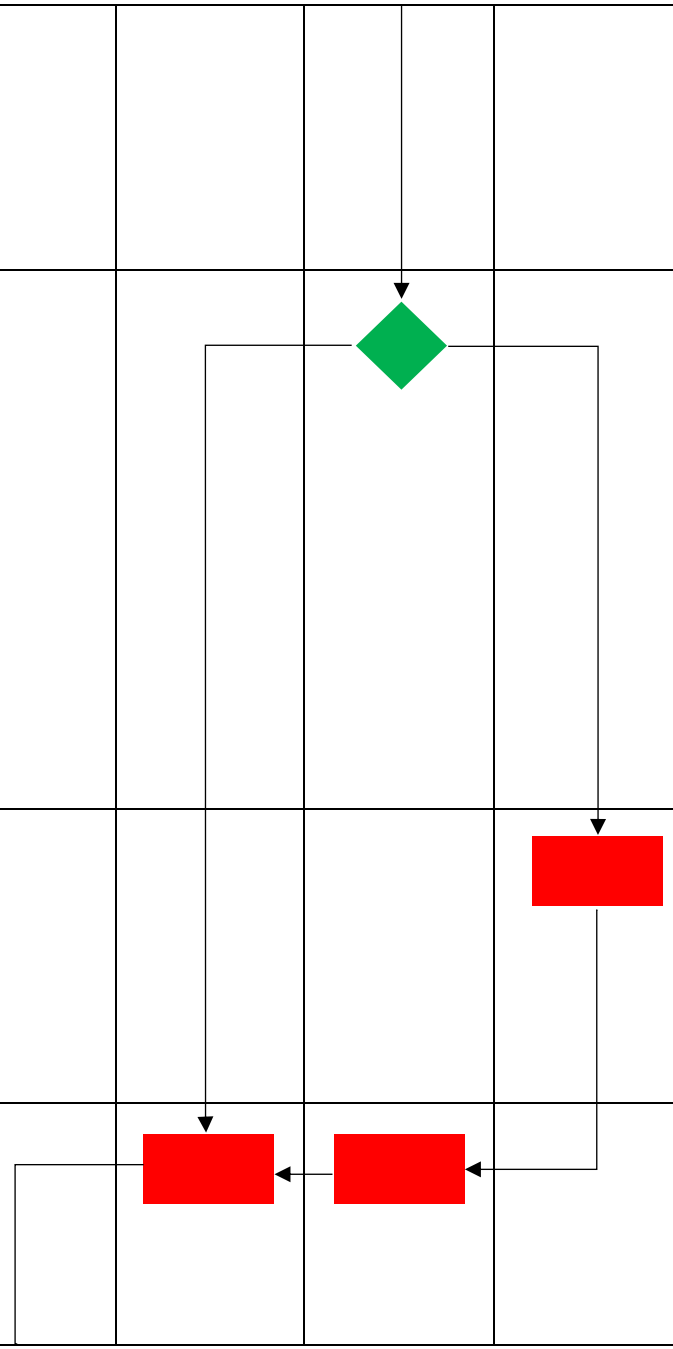
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA KANTOR WILAYAH NUSA TENGGARA TIMUR DIVISI ADMINISTRASI	NOMOR SOP	: W22.OT.02.02-
	TANGGAL PEMBUATAN	: 31 Oktober 2022
	TANGGAL REVISI	:
	TANGGAL EFEKTIF	: 31 Oktober 2022
	DISAHKAN OLEH	Kepala Kantor Wilayah  Marciana Dominika Jone NIP 196411261991032001
	Nama SOP	: Penanganan Insiden Keamanan Jaringan

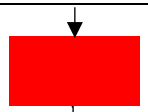
DASAR HUKUM:	KUALIFIKASI PELAKSANA:
a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; b. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik; c. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik; d. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik; e. Keputusan Menteri Hukum dan Hak Asasi Manusia Nomor M.HH-01.TI.06.02 Tahun 2017 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.	1. Memiliki tanggung jawab dan kewenangan hak akses dalam aplikasi; 2. Memiliki kemampuan dalam penggunaan akun pada aplikasi tersebut; 3. Memahami mekanisme pemeliharaan sesuai dengan ketentuan yang berlaku.
KETERKAITAN:	PERALATAN/PERLENGKAPAN:
	1. Perangkat Pengolah Data; 2. Jaringan Internet; 3. Jaringan Telekomunikasi; 4. Tata Naskah Dinas; 5. Akses Aplikasi
PERINGATAN:	PENCATATAN DAN PENDATAAN:
Apabila SOP ini tidak dilaksanakan maka akan berdampak pada terlambatnya penanganan terhadap insiden keamanan jaringan sehingga pelayanan yang berbasis sistem informasi tidak bisa berjalan dengan baik.	Disimpan sebagai data elektronik dan manual.

STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN KEAMANAN JARINGAN

No	Kegiatan	Pelaksana					Mutu Baku			Ket.
		Pelaksana Teknis	Kasub HRBTI	Kabag Program dan HUMAS	Kadiv Administrasi	Kakanwil	Keterangan	Waktu	Output	
1.	Melakukan pemantauan lalu lintas jaringan dan analisa log dan rekam digital lainnya pada jaringan	Mulai					Jaringan internet dan intranet	60 Menit	Dokumen pemantauan jaringan yang berisi: a. Konfigurasi b. Lalu lintas normal (baseline) jaringan c. Performa jaringan	
2.	Memeriksa/mendeteksi dan menemukan celah keamanan yang menjadi penyebab insiden apabila terdapat anomali pada jaringan						Dokumen pemantauan jaringan yang berisi: a. Konfigurasi b. Lalu lintas normal (baseline) jaringan c. Performa jaringan	3 Jam	Dokumen hasil pemeriksaan setelah deteksi berisi daftar anomali jaringan	
3.	Melakukan klasifikasi tingkatan insiden meliputi penilaian dampak dan prioritas insiden keamanan jaringan serta membuat dokumen						Dokumen hasil pemeriksaan setelah deteksi berisi daftar anomali jaringan	60 Menit	1. Dokumen hasil klasifikasi tingkatan insiden jaringan; 2. Dokumen gangguan keamanan jaringan	

									yang berisi dampak dan prioritas insiden keamanan jaringan	
4.	Melakukan eskalasi insiden berdasarkan klasifikasi insiden keamanan jaringan dan/atau memberikan arahan terkait penanganan keamanan jaringan						1. Dokumen hasil klasifikasi tingkatan insiden jaringan; 2. Dokumen gangguan keamanan jaringan yang berisi dampak dan prioritas insiden keamanan jaringan	30 Menit	Dokumen insiden keamanan jaringan yang berisi dampak dan prioritas insiden keamanan jaringan	Merujuk kepada tingkat klasifikasi insiden yang telah ditetapkan Y = kritikal T = ringan dan sedang
5.	Menerima dokumen gangguan keamanan jaringan dan memberikan arahan						Laporan insiden keamanan jaringan yang berisi dampak dan prioritas insiden keamanan jaringan	15 Menit	Disposisi arahan penyelesaian insiden keamanan jaringan	
6.	Disposisi penanggulangan dan pemulihan insiden jaringan secara cepat dan tepat						Disposisi arahan penyelesaian insiden keamanan jaringan	1 Hari	Disposisi laporan insiden	



7.	Melakukan tindakan korektif untuk menanggulangi insiden jaringan serta melakukan perbaikan celah keamanan (*hardening*) untuk mencegah insiden terulang kembali						Disposisi laporan insiden	3 Jam	1. Draft laporan penanggu-langan insiden keamanan jaringan 2. Check List 3. Bukti penanggu-langan insiden keamanan jaringan	
8.	Memeriksa dan menyetujui laporan penanggulangan						1. Draft laporan penanggu-langan insiden keamanan jaringan 2. Check List 3. Bukti penanggu-langan insiden keamanan jaringan	30 Menit	Dokumen penanggula-ngan insiden keamanan	