KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA PUSAT DATA DAN TEKNOLOGI INFORMASI		
	NOMOR SOP	KHH. X.1 c. 3e. 9
	TANGGAL PEMBUATAN	22 SEPTEMBER 2020
	TANGGAL REVISI	
	TANGGAL EFEKTIF	23 NOVEMBER 2020
	DISAHKAN OLEH	**SEKRETARIS JENDERAL** **Dr. BAMBANG RANTAM SARIWANTO** **NIP 19601215 198802 1 001**
	NAMA SOP :	**Penanganan Insiden Keamanan Jaringan**

DASAR HUKUM :	**KUALIFIKASI PELAKSANA :**
1 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik 2 Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik 3 Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik 4 Peraturan Pemerintah Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik 5 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 PENDAFTARAN :**
Apabila SOP tidak dilaksanakan maka akan berdampak pada terlambatnya penanganan terhadap insiden keamanan jaringan sehingga pelayanan yang berbasis sistem informasi tidak bisa berjalan dengan baik	Di simpan sebagai data elektronik dan manual jika suatu saat diperlukan kembali

SOP Penanganan Insiden Keamanan Jaringan

No.	Aktivitas	Pelaksana				Mutu Baku			Keterangan
		Pelaksana Teknis	Kepala Subbidang Pemeliharaan TI/ Pengamanan Data dan Jaringan	Kepala Bidang Data dan Pengamanan Jaringan	Kepala Pusat Data dan Teknologi Informasi	Kelengkapan	Waktu	Output	
1	Melakukan pemantauan lalu lintas jaringan dan analisa log & 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 di 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. 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 dan menemukan celah keamanan yang menjadi penyebab insiden serta melakukan perbaikan celah keamanan *(hardening)* untuk mencegah insiden terulang kembali					Disposisi laporan insiden	3 jam	1. Draft Laporan Penanggulangan insiden keamanan jaringan 2. Check List 3. Bukti penanggulangan insiden keamanan jaringan	
8	Memeriksa dan menyetujui laporan penanggulangan				Selesai	1. Draft Laporan Penanggulangan insiden keamanan jaringan 2. Check List 3. Bukti penanggulangan insiden keamanan jaringan	30 menit	Dokumen Penanggulangan Insiden Keamanan Jaringan	

