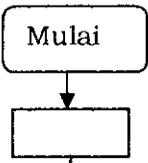
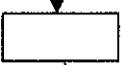
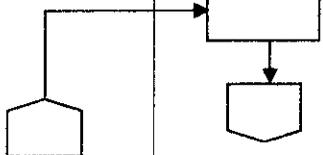


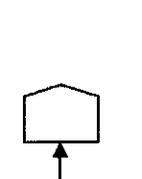
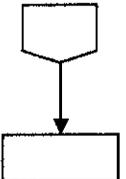
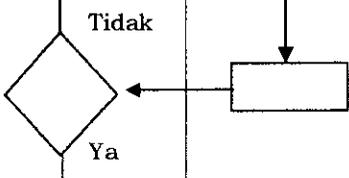
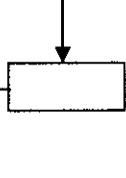
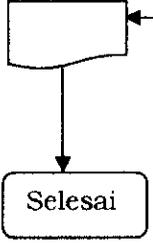


PEMERINTAH KABUPATEN LUMAJANG
DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN LUMAJANG
BIDANG APLIKASI INFORMATIKA

NOMOR SOP	427.53/4/2.09/2021
TANGGAL PEMBUATAN	23 MEI 2021
TANGGAL REVISI	
TANGGAL PENGESAHAN	
DISAHKAN OLEH	<p>KEPALA DINAS KOMUNIKASI DAN INFORMATIKA YOGA PRATOMO, S.STP NIP. 19780910 199802 1 001</p>
NAMA SOP	SOP INCIDENT HANDLING KEAMANAN WEB DAN APLIKASI

DASAR HUKUM	KUALIFIKASI PELAKSANA
<ol style="list-style-type: none"> 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 96 tahun 2012 tentang pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik 5. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 15 tahun 2014 tentang Pedoman Standard Pelayanan 6. Peraturan Daerah Nomor 8 tahun 2016 tentang Pelayanan Publik 7. Peraturan Daerah Nomor 16 tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah 8. Peraturan Bupati Lumajang Nomor 7 tahun 2021 tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika 	<ol style="list-style-type: none"> 1. Kepala Bidang Aplikasi Informatika (APTIKA) 2. Kepala Seksi Pengelolaan dan Pengembangan Infrastruktur SPBE 3. Administrator Jaringan 4. Programmer
KETERKAITAN	PERALATAN/PERLENGKAPAN
	<ol style="list-style-type: none"> 1. Komputer 2. Printer 3. ATK
PERINGATAN	PENCATATAN DAN PENDATAAN
<ol style="list-style-type: none"> 1. Pelaksana bertanggungjawab atas pelaksanaan aktivitas yang telah dibakukan dan ditetapkan 2. Segala bentuk penyimpangan atas mutu baku terkait perlengkapan waktu maupun output dikategorikan sebagai bentuk kegagalan yang harus dipertanggungjawabkan oleh pelaksana 	<ol style="list-style-type: none"> 1. Pencatatan Kondisi Perangkat Data Center

No	Aktivitas	Pelaksana			Mutu Baku			Keterangan
		Kepala Bidang Aplikasi dan Informatika	Kepala Seksi Pengelolaan dan Pengembangan Infrastruktur Sistem Pemerintahan Berbasis Elektronik	Administrator Jaringan dan Programmer	Persyaratan/Kelengkapan	Waktu	Output	
1.	Memastikan dan Mengidentifikasi Insiden				<ul style="list-style-type: none"> - Komputer / Laptop - Jaringan Internet - Log akses (<i>modsec webservice</i>) 	1 Jam	Informasi Detail insiden	Waktu penyelesaian menyesuaikan tingkat kesulitan insiden
2.	Tahapan <i>Containment</i> dengan melakukan <i>backup</i> seluruh data aplikasi termasuk file sistem dan database, mencari dan menemukan sumber serangan, memutus koneksi dengan sumber penyerang, <i>scanning script</i> malware / <i>backdoor</i>				<ul style="list-style-type: none"> - Komputer / Laptop - Jaringan Internet - Informasi detail insiden - Dokumen Pengetahuan - <i>Backup server</i> 	4 Jam	Hasil backup, serangan dapat dihentikan, hasil scanning system	
3.	Tahapan <i>Eradication</i> dengan melakukan penghapusan semua konten yang terinfeksi malware (<i>backdoor, rootkit</i>), menghapus konten web yang terdapat celah keamanan.				<ul style="list-style-type: none"> - Komputer / Laptop - Jaringan Internet - Informasi detail insiden - Dokumen Pengetahuan - Hasil Scanning Sistem 	1 Jam	Server web/aplikasi bersih dari malware	Waktu penyelesaian menyesuaikan tingkat kesulitan insiden

<p>5. Tahapan <i>Recovery</i> dengan melakukan patching aplikasi dan <i>server</i>, menutup semua kerentanan yang telah diketahui, dan mengupload ulang aplikasi dan sistem baru yang telah di perbarui.</p>				<ul style="list-style-type: none"> - Komputer / Laptop - Jaringan Internet - Dokumen Pengetahuan - Hasil Scanning Sistem - Hasil backup 	<p>4 Jam</p>	<p>System dan aplikasi yang telah terupdate</p>	<p>Waktu penyelesaian menyesuaikan tingkat kesulitan insiden</p>
<p>6. <i>Penetration Testing</i></p>				<ul style="list-style-type: none"> - Komputer / Laptop - Jaringan Internet 	<p>1 Jam</p>	<ul style="list-style-type: none"> - Hasil pentest - Laporan hasil penanganan insiden 	
<p>7. Informasi hasil penanganan insiden</p>				<ul style="list-style-type: none"> - Laporan hasil penanganan insiden 	<p>1 Jam</p>	<p>Laporan hasil penanganan insiden</p>	