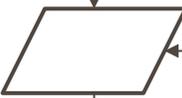




PEMERINTAH KABUPATEN BATANG
DINAS KOMUNIKASI DAN INFORMATIKA

	NOMOR SOP	555/0966/2024
	TGL. PEMBUATAN	9 MARET 2024
	TGL. REVISI	
	TGL. EFEKTIF	10 MARET 2024
	DISAHKAN OLEH	 TRIOSSY JUNIARTO, SIP, MM NIP. 196906211990031003
	NAMA SOP	PROSEDUR BAKU PENANGANAN INSIDEN MALWARE
DASAR HUKUM	KUALIFIKASI PELAKSANA	
<ol style="list-style-type: none">Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.Peraturan Menteri Dalam Negeri Nomor 52 tahun 2011 tentang Standar Operasional Prosedur di lingkungan Pemerintah Provinsi dan Kabupaten/Kota.Peraturan Menteri PANRB Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur (SOP) Administrasi Pemerintahan.Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2023 tentang Interoperabilitas Data Penyelenggaraan Sistem pemerintahan Berbasis Elektronik Dan Satu Data Indonesia.Peraturan BSSN Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah.Peraturan Bupati Batang Nomor 50 Tahun 2019 tentang Penyelenggaraan SPBE di Lingkungan Pemerintah Kabupaten Batang.	<ol style="list-style-type: none"><ol style="list-style-type: none">Memahami konsep dasar sistem;Operasional TIK;Memahami konsep dasar keamanan siberMemahami dasar sistem jaringan telekomunikasi;Memahami sistem administrasi keamanan informasi dan persandian;Memiliki pengetahuan tentang <i>malware</i>, termasuk <i>virus</i>, <i>worm</i>, <i>ransomware</i>, <i>spyware</i>Memahami penggunaan <i>Tools</i> untuk <i>Penetration Testing</i>;Mampu mengoperasikan <i>Tools</i> untuk <i>Penetration Testing</i>;Bekerja di Dinas Komunikasi dan Informatika Kabupaten Batang	
KETERKAITAN	PERALATAN/PERLENGKAPAN	
<ol style="list-style-type: none">Prosedur ini berkaitan dengan keamanan sistem informasi di Pemerintah Kabupaten Batang	<ol style="list-style-type: none"><ol style="list-style-type: none">Jaringan InternetKomputer/LaptopAplikasi	
PERINGATAN	PENCATATAN DAN PENDATAAN	
Apabila prosedur tidak dilaksanakan maka kerusakan akan lebih meluas dan merugikan yang terdampak		Disimpan sebagai data elektronik dan manual

I. PROSEDUR PENANGANAN INSIDEN SERANGAN MALWARE

No	Aktivitas Kegiatan	Pelaksana		Mutu Baku			Keterangan
		Pemohon	Tim Teknis	Kelengkapan	Waktu	Output	
1	Menerima laporan aduain insiden			Laporan (digital/tertulis)	5 menit	Laporan insiden	
2	Identifikasi dan Analisis adanya <i>malware</i> (memeriksa <i>antivirus</i> , identifikasi file yang tidak dikenal pada root atau <i>system directory</i> , memeriksa <i>service</i> yang berjalan)			<ul style="list-style-type: none"> - <i>Log file</i> - <i>Bash history</i> - Aplikasi <i>text editor</i> - Laptop/Komputer 	120 menit	Catatan hasil identifikasi dan analisa	
3	Containment (Mencegah penyebaran <i>malware</i>)			Laptop/Komputer	90 menit	Informasi Dokumentasi perubahan file, log, dan sumber serangan	
4	Eradication (menganalisa dan menghapus <i>malware</i> dari sistem)			Laptop/Komputer	90 menit	List <i>malware</i> yang dihapus	
5	Pemulihan (validasi sistem, monitoring aktivitas <i>traffic</i> , melakukan <i>patching</i> sistem dan <i>hardening</i> sistem)			Laptop/Komputer	24 Jam		Jika pada proses pemulihan masih terdapat <i>malware</i> atau gangguan, maka kembali ke identifikasi dan analisis
6	Dokumentasi dan Pembuatan Laporan Post Insiden			Laptop/Komputer, Dokumen Laporan	45 menit	Dokumen Laporan digital/manual	
7	Selesai						