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	KEPALA DISKOMINFO KAB. BATANG **TRIOSSY JUNIARTO, SIP, MM** NIP. 196906211990031003
		NAMA SOP	PROSEDUR BAKU PENANGANAN INSIEDEN MALWARE

DASAR HUKUM		KUALIFIKASI PELAKSANA
1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. 2. Peraturan Menteri Dalam Negeri Nomor 52 tahun 2011 tentang Standar Operasional Prosedur di lingkungan Pemerintah Provinsi dan Kabupaten/Kota. 3. Peraturan Menteri PANRB Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur (SOP) Administrasi Pemerintahan. 4. Peraturan Menteri Komunikasi dan Informatika Nomor 1 Tahun 2023 tentang Interoperabilitas Data Penyelenggaraan Sistem pemerintahan Berbasis Elektronik Dan Satu Data Indonesia. 5. Peraturan BSSN Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah. 6. Peraturan Bupati Batang Nomor 50 Tahun 2019 tentang Penyelenggaraan SPBE di Lingkungan Pemerintah Kabupaten Batang.	1.	a. Memahami konsep dasar sistem; b. Operasional TIK; c. Memahami konsep dasar keamanan siber d. Memahami dasar sistem jaringan telekomunikasi; e. Memahami sistem administrasi keamanan informasi dan persandian; f. Memiliki pengetahuan tentang *malware*, termasuk *virus, worm, ransomware, spyware* g. Memahami penggunan *Tools* untuk *Penetration Testing*; h. Mampu mengoperasikan *Tools* untuk *Penetration Testing*; i. Bekerja di Dinas Komunikasi dan Informatika Kabupaten Batang

KETERKAITAN		PERALATAN/PERLENGKAPAN
1. Prosedur ini berkaitan dengan keamanan sistem informasi di Pemerintah Kabupaten Batang	1.	1. Jaringan Internet 2. Komputer/Laptop 3. Aplikasi

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 *malware* (memeriksa *antivirus,* identifikasi file yang tidak dikenal pada root atau *system directory*, memeriksa *service* yang berjalan)			- *Log file* - *Bash history* - Aplikasi *text editor* - Laptop/Komputer	120 menit	Catatan hasil identifikasi dan analisa	
3	Containment (Mencegah penyebaran *malware*)			Laptop/Komputer	90 menit	Informasi Dokumentasi perubahan file, log, dan sumber serangan	
4	Eradication (menganalisa dan menghapus malware dari sistem)			Laptop/Komputer	90 menit	List *malware* yang dihapus	
5	Pemulihan (validasi sistem, monitoring aktivitas *traffic*, melakukan *patching* sistem dan *hardening* sistem			Laptop/Komputer	24 Jam		Jika pada proses pemulihan masih terdapat *malware* 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