DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN TAPIN

Nomor SOP	000.6/143/Diskominfo/VII/2025
Tanggal Pembuatan	29 Juli 2025
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	Kepala Dinas Komunikasi dan Informatika Kabupaten Tapin **WAHYUDI PRANOTO, S.Sos., MT** Pembina Tk I / IV/b NIP. 19710130 199303 1 005
Nama SOP	Penetration Testing / Information Technology Security Assessment (ITSA)

Dasar Hukum :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
2. Undang-Undang Nomor 72 Tahun 2022 tentang Infrastruktur Informasi Vital
3. Peraturan Presiden No.95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (SPBE) Pasal 40 dan 41 (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182).
4. Peraturan Kepala BSSN No. 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik
5. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber
6. Peraturan Kepala BSSN No. 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis ELektronik
7. Peraturan Daerah Kabupaten Tapin Nomor 10, Tahun 2019 Tentang Perubahan Atas Peraturan Daerah Kabupaten Tapin Nomor 09 Tahun 2016 Tentang Pembentukan Dan Susunan Perangkat Daerah Kabupaten Tapin
8. Peraturan Bupati Tapin No. 16 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
9. Surat Keputusan Bupati Tapin No. 250 Tahun 2023 tentang Tim Tanggap Insiden Siber (Computer Security Incident Response Team)

Keterkaitan :

1. Lintas SKPD Pemerintah Kabupaten Tapin
2. Lintas Kompenen

Peringatan :

1. Apabila kegiatan Information Technology Security Assessment (ITSA) tidak dilakukan sesuai prosedur, maka pengamanan aplikasi tidak dapat dicapai secara optimal;
2. Kegiatan Information Technology Security Assessment (ITSA) bersifat tertutup/terbatas sesuai kebutuhan dan/atau permintaan

Kualifikasi Pelaksana :

1. Memahami Tugas Pokok dan Fungsi Dinas Komunikasi dan Informatika;
2. Memahami konsep dasar sistem operasional TIK;
3. Memahami dasar sistem jaringan telekomunikasi;
4. Memahami sistem dasar administrasi persandian dan keamanan informasi;
5. Memahami penggunaan tools untuk penetration testing;
6. Mampu mengoperasionalkan tools untuk penetration testing;
7. Bekerja pada unit teknis yang menangani persandian.

Peralatan / Perlengkapan :

1. Komputer (PC), Printer;
2. Jaringan Internet
3. Alat Komunikasi;
4. Tool Kit.

Pencatatan dan Pendataan :

1. Kegiatan Information Technology Security Assessment (ITSA) merupakan kegiatan audit keamanan sistem informasi untuk pengamanan informasi san sister elektronik;
2. Kegiatan Security Assessment merupakan kegiatan terbatas atas perintah pimpinan SKPD.

Penyelenggaraan Pelayanan Penilaian Keamanan Sistem Informasi (Information Technology Security Assessment (ITSA))
Pada Dinas Komunikasi dan Informatika Kabupaten Tapin

NO	Uraian	Pelaksana				Mutu Baku			Ket
		Kadis	Kabid	JFT. Sandiman /Penyetaraan Kasi	Pelaksana	Persyaratan/Kelengkapan	Waktu	Output	
1	Menerima Surat Permohonan dukungan Kerjasama Information Technology Security Assessment (ITSA) dari pihak membutuhkan yang selanjutnya memberikan disposisi kepada Kepala Bidang Persandian dan Statistik					a. Surat; b. Lembar disposisi c. Komputer/Laptop d. Alat Komunikasi	5 Menit	a. Surat Permohonan; b. Disposisi	
2	Kepala Bidang Persandian dan Statistik meneruskan disposisi Kepala Dinas kepada kepada Kepala Seksi Persandian/JFT. Sandiman					a. Surat; b. Lembar disposisi	3 Menit	a. Surat; b. Disposisi c. Agenda	
3	Kepala Seksi Persandian menyiapkan tim teknis pelaksanaan Information Technology Security Assessment (ITSA)					a. Disposisi; b. Agenda; c. Komputer/Laptop;	10 Menit	a. Disposisi; b. Agenda; c. Komputer/Laptop; d. SDM.	
4	Tim Teknis melakukan identifikasi awal aplikasi dan sistem yang akan di test					a. Disposisi; b. Agenda;	4 Jam	Identifikasi awal aplikasi dan sistem yang akan di test	
5	Pelaksanaan kegiatan Information Technology Security Assessment (ITSA) terhadap Aplikasi dan Sistem yang menjadi objek audit					a. Komputer/Laptop; b. Pentest Tools; c. Jaringan;	5 Hari	Data hasil audit	
6	Penyusunan laporan hasil analisis keamanan hasil dari proses Information Technology Security Assessment (ITSA)					a. Komputer/Laptop; b. Kertas;	4 Jam	Laporan hasil analisis	
7	Penyusunan laporan hasil akhir kegiatan/ rekomendasi Information Technology Security Assessment (ITSA)					a. Komputer/Laptop; b. Printer;	6 Jam	Laporan hasil kegiatan	
8	Penyampaian laporan hasil kegiatan Information Technology Security Assessment (ITSA)						30 Menit	Dokumen hasil kegiatan