[LAMBANG KABUPATEN]

PEMERINTAH KABUPATEN ACEH TENGAH

DINAS KOMUNIKASI DAN INFORMATIKA

Jalan Tunas Harapan No. 1 Takengon 24514

INSTRUMEN SELF-ASSESSMENT

INDEKS KEMATANGAN KEAMANAN SIBER DAN PERSANDIAN (IKASANDI)

AREA KEAMANAN SIBER

KABUPATEN ACEH TENGAH

TAHUN 2026

Nama Instansi	Pemerintah Kabupaten Aceh Tengah	
Cakupan Penilaian	Tata kelola & penyelenggaraan keamanan siber (Dinas Kominfo dan PD terkait)	
Dasar Acuan	PermenPANRB No. 8 Tahun 2026; Peraturan BSSN tentang IKASANDI; Perbup 6/2025	
Periode Penilaian	Semester I Tahun 2026	
Tanggal Pengisian	15 Juni 2026	
Penanggung Jawab	Kepala Dinas Komunikasi dan Informatika	
Pengisi	Tim Penilai (Diskominfo Bidang Persandian & Keamanan Informasi)	
Nama Portal	Portal IKASANDI BSSN (https://ikasandi.bssn.go.id)	

A. Petunjuk Pengisian

Instrumen ini mengacu pada kerangka Indeks Kematangan Keamanan Siber dan Persandian (IKASANDI) yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), khususnya Area Keamanan Siber. Setiap butir pernyataan dinilai dengan Skor Kematangan 0—5 sebagai berikut:

Skor	Sebutan	Penjelasan
0	Tidak Ada	Tidak ada kegiatan/kontrol

		sama sekali.
1	Initiate / Rintisan	Kegiatan/kontrol sudah ada dalam skala terbatas/dasar dan belum terdokumentasi penuh.
2	Emerging / Berkembang	Kegiatan/kontrol sudah dilaksanakan sebagian terdokumentasi.
3	Established / Mapan	Kegiatan/kontrol telah baku, dilaksanakan dan terdokumentasi menyeluruh.
4	Leading / Terkelola	Dievaluasi, diukur, dan ditingkatkan secara berkelanjutan.
5	Transformative	Menjadi rujukan/best practice dan berinovasi berkelanjutan.

Isilah kolom "Skor" dengan angka 0—5 sesuai kondisi aktual di Pemkab Aceh Tengah. Kolom "Bukti Awal" berisi keterangan/dokumen pendukung yang dilampirkan pada saat reviu.

B. Kerangka Area Keamanan Siber

Berdasarkan kerangka IKASANDI, Area Keamanan Siber dinilai dari 5 (lima) domain/kategori sebagai berikut:

Kode	Domain/Kategori	Bobot
KS-1	Tata Kelola Keamanan Siber	20%
KS-2	Identifikasi & Manajemen Risiko	18%
KS-3	Proteksi & Kontrol Keamanan	22%
KS-4	Deteksi & Pemantauan	18%
KS-5	Respon & Pemulihan Insiden	22%

C. Daftar Butir Instrumen per Domain

KS-1 — Tata Kelola Keamanan Siber

No.	Butir Penilaian	Skor (0—5)	Bukti Awal / Keterangan
1	Tersedianya dasar hukum/kebijakan keamanan siber di daerah (mis. Perbup 6/2025).	1	
2	Ditetapkannya struktur/peran keamanan siber di Diskominfo (Bidang Persandian &	1	

	Keamanan Informasi).		
3	Adanya komitmen pimpinan dalam penyelenggaraan keamanan siber.	1	
4	Tersedianya anggaran untuk penyelenggaraan keamanan siber.	1	
5	Dilakukannya koordinasi dengan BSSN/Komdigi/CSIRT/ POLDA terkait keamanan siber.	1	
6	Dilakukannya sosialisasi/penyadaran keamanan siber secara terbatas.	1	

KS-2 — Identifikasi & Manajemen Risiko

No.	Butir Penilaian	Skor (0—5)	Bukti Awal / Keterangan
1	Tersedianya inventaris aset TIK (perangkat, aplikasi, data) di tingkat dasar.	1	
2	Dilakukannya identifikasi awal terhadap aset kritikal/Infrastruktur Informasi Vital (IIV).	1	
3	Dilakukannya penilaian risiko keamanan siber secara sederhana/tahunan.	1	
4	Tersedianya daftar vendor/pihak ketiga yang mengakses sistem dan diketahui risikonya.	1	
5	Adanya pendataan kerentanan (vulnerability) yang pernah terjadi/ditemukan.	1	

KS-3 — Proteksi & Kontrol Keamanan

No.	Butir Penilaian	Skor (0—5)	Bukti Awal / Keterangan
1	Diterapkannya kontrol akses dasar (username/password) pada aplikasi/sistem.	1	
2	Diterapkannya kebijakan password dan/atau otentikasi multi-faktor (MFA)	1	

	pada akun penting.		
3	Dipasangnya firewall/sistem pengamanan jaringan pada gateway internet.	1	
4	Diterapkankan proteksi antivirus/anti-malware pada perangkat end user/server.	1	
5	Dilakukannya pembaruan/patch sistem secara manual/berkala pada sistem utama.	1	
6	Diterapkannya enkripsi pada koneksi (HTTPS) dan/atau data penting.	1	
7	Dilakukannya backup data secara rutin (belum tentu teruji restorasi).	1	
8	Diterapkannya kebijakan pembatasan hak akses (least privilege) pada akun administrator.	1	

KS-4 — Deteksi & Pemantauan

No.	Butir Penilaian	Skor (0—5)	Bukti Awal / Keterangan
1	Diaktifkannya pencatatan log (logging) pada server/aplikasi utama.	1	
2	Dilakukannya pemantauan ketersediaan layanan (uptime) secara manual/dashboard dasar.	1	
3	Dipasangnya sistem deteksi awal (antivirus/SNMP/monitor bandwidth).	1	
4	Ditetapkannya kontak person/petugas yang dapat dihubungi jika terjadi gangguan.	1	
5	Adanya mekanisme internal pelaporan insiden dari pegawai ke tim TIK.	1	

KS-5 — Respon & Pemulihan Insiden

No.	Butir Penilaian	Skor (0—5)	Bukti Awal /

			Keterangan
1	Tersedianya SOP/prosedur awal penanganan insiden siber.	1	
2	Ditetapkannya Tim Tanggap Insiden Siber (TTIS/CSIRT) tingkat daerah (SK dalam proses/telah ditetapkan).	1	
3	TTIS/CSIRT telah teregistrasi/berkoordinasi dengan CSIRT nasional (BSSN).	1	
4	Dilakukannya penanganan insiden sederhana dalam 12 bulan terakhir.	1	
5	Dilakukannya pencatatan insiden (waktu, jenis, dampak, penanganan) pada log/register.	1	
6	Adanya rencana pemulihan sederhana dan backup data untuk pemulihan layanan.	1	

D. Rekapitulasi Skor per Domain

Kode	Domain	Skor Rata-rata	Level Kematangan	Skor Terbobot
KS-1	Tata Kelola Keamanan Siber	1.17	Initiate	0.23
KS-2	Identifikasi & Manajemen Risiko	1.00	Initiate	0.18
KS-3	Proteksi & Kontrol Keamanan	1.13	Initiate	0.25
KS-4	Deteksi & Pemantauan	1.00	Initiate	0.18
KS-5	Respon & Pemulihan Insiden	1.17	Initiate	0.26
	SKOR TOTAL IKASANDI AREA KEAMANAN SIBER	1.10	INISIATE (1)	1.10

Dengan skor total 1,10 (pada rentang 0 — <1,50), nilai IKASANDI Area Keamanan Siber Pemerintah Kabupaten Aceh Tengah tahun 2026 berada pada Level 1 — Initiate.

E. Kesimpulan Sementara dan Catatan

- Kebijakan keamanan siber telah memiliki payung (Perbup 6/2025) dan struktur unit;
- Kontrol dasar (firewall, antivirus, password, HTTPS, backup) sudah berjalan pada layanan utama;
- Tata kelola, SOP formal, pengukuran risiko, monitoring terotomasi, uji pemulihan, dan registrasi CSIRT perlu ditingkatkan;
- Sebagai pembanding, hasil pengukuran Indeks KAMI 5.0 pada Area Keamanan Siber memperoleh skor 563 (skala 0—1000);
- Rencana peningkatan menuju Level 2 (Emerging) difokuskan pada penetapan SOP, identifikasi IIV, pelaporan insiden, dan pelatihan.

Takengon, 15 Juni 2026

Kepala Dinas Komunikasi dan Informatika

(.....)

NIP. .....