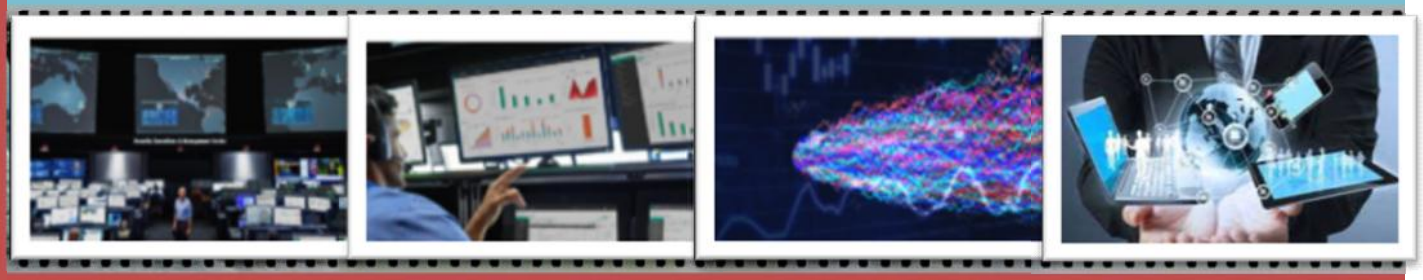
LAPORAN AKHIR

KEGIATAN PENYELENGGARAAN PERSANDIAN DAN KEAMANAN INFORMASI DAERAH TAHUN 2018

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN PESISIR SELATAN



TAHUN 2018

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji syukur kita panjatkan kehadirat Allah SWT atas terlaksananya Kegiatan Penyelenggaraan Persandian dan keamanan Informasi Daerah Tahun 2018, dengan tersusunnya laporan akhir kegiatan tersebut pada Dinas Komunikasi dan Informasi Kabupaten Pesisir Selatan.

Laporan akhir kegiatan ini berisi laporan tentang pelaksanaan Kegiatan Penyelenggaraan Persandian dan keamanan Informasi Daerah Tahun 2018 mulai dari tahap persiapan sampai kegiatan ini selesai dilaksanakan.

Akhir kata, kami mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam pelaksanaan kegiatan ini.

Wassalamu'alaikum Warohmatullohi Wabarokatuh.

Painan, Desember 2018

Kepala Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan,

PEMERINTAH KABUPATEN PESISIR SELATAN
DINAS KOMUNIKASI DAN INFORMATIKA

JUNAIDI, S.Kom, M.E
Pembina Tk.I /IV(b)
NIP. 19700609 199703 1 002

BAB I
PENDAHULUAN

I.1. Latar Belakang

Masalah Keamanan Informasi telah mengalami banyak perubahan selama 8 tahun terakhir sejak versi SNI ISO: IEC 27001:2005 karena perubahan teknologi baru, peluang bisnis yang makin luas dengan memanfaatkan teknologi informasi (TI), serta ancaman dan kerentanan baru yang muncul menyertai penggunaan TI. Agar standar sistem manajemen keamanan informasi tetap sesuai dengan perubahan yang terjadi dalam lingkungan yang terkait penggunaan TI, maka harus juga dilakukan perubahan atau revisi terhadap versi sebelumnya.

Penerapan dan Pemenuhan *Indeks KAMI bagi Penyelenggara Pelayanan* Publik ini disusun berdasarkan standar SNI ISO : IEC 27001 : 2013 yang telah dirilis oleh *International Organization for Standardization* (ISO)/Organisasi Standarisasi Internasional pada bulan Oktober 2013 dan diratifikasi oleh Badan Standar Nasional Republik Indonesia. *Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik* yang telah diterbitkan Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika (Kominfo) pada tahun 2011.

Sebagaimana sudah banyak diketahui, khususnya bagi penyelenggara pelayanan publik di lingkungan Kementerian/ Lembaga, baik pusat maupun daerah, sejak tahun 2008 Kominfo telah menyelenggarakan sosialisasi dalam bentuk bimbingan teknis (Bimtek) tentang keamanan informasi untuk meningkatkan kesadaran dan kepedulian setiap individu yang terlibat dalam penyelenggaraan pelayanan publik. Selain menjelaskan persyaratan standar SNI ISO: IEC 27001, Bimtek juga mensimulasikan penilaian secara mandiri *(self assessment)* tingkat kesiapan dan kematangan sistem manajemen keamanan informasi dengan mengisi pertanyaan-pertanyaan yang dirangkum dalam alat bantu penilaian yang disebut **Indeks KAMI.**

Pasca keikutsertaan dalam Bimtek, setiap penyelenggara pelayanan publik kemudian juga didorong untuk mengikuti penilaian tingkat. Kesiapan pengamanan informasi melalui kegiatan pemeriksaan dokumen *(desktop assessment)* dan verifikasi dan pemeriksaan penerapan *(on-site assessment)* oleh asesor independen yang telah menjadi program tahunan Direktorat Keamanan

Informasi Kominfo.

Dengan terbitnya Peraturan Menteri Komunikasi dan informatika (Kominfo) nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI), maka keharusan untuk memiliki dan menerapkan SMKI lebih ditekankan kembali bagi pelayanan publik khususnya yang berkategori "Tinggi" dan "Strategis".

Buku ini juga memuat kebijakan dan prosedur utama yang diperlukan untuk menyusun sistem manajemen keamanan informasi (SMKI) sesuai persyaratan standar SNI ISO:IEC 27001:2013.

I.2. Tujuan

Panduan Penerapan dan Pemenuhan Indeks KAMI ini disusun utamanya untuk membantu Penyelenggara Pelayanan Publik dalam menyusun sistem dokumentasi SMKI yang memadai dan memenuhi persyaratan standar SNI ISO: IEC 27001: 2013. Beberapa tujuan lainnya antara lain:

1. Mampu melakukan kajian risiko terkait penggunaan TI dan melakukan tata kelola keamanan informasi secara efektif, efisien, dan konsisten sesuai hasil kajian risiko;
2. Mampu melakukan penilaian mandiri (self-assesment) secara objektif dengan menggunakan Indeks Keamanan Informasi (Indeks KAMI);
3. Mampu menyusun sistem dokumentasi minimum yang diperlukan untuk menerapkan tata kelola keamanan informasi;
4. Memahami metode, tahapan dan langkah-langkah untuk menyusun dan menerapkan SMKI.

I.3. Ruang Lingkup Penerapan

Panduan ini direkomendasikan untuk diterapkan di lingkungan organisasi penyelenggara pelayanan publik terdiri dari OPD dan Nagari. Dalam Peraturan Menteri Kominfo Nomor 4 Tahun 2016 disebutkan bahwa Penyelenggara Pelayanan Publik yang dicakup dapat meliputi:

1. Institusi penyelenggara pemerintahan dan/atau Satuan Kerja Penyelenggara di lingkungannya;
2. Korporasi berupa Badan Usaha Milik Daerah dan/atau Satuan Kerja Penyelenggara di lingkungannya;

3. Lembaga independen yang dibentuk berdasarkan Undang-Undang dan/atau Satuan Kerja Penyelenggara di lingkungannya; atau
4. Badan hukum lain yang menyelenggarakan Pelayanan Publik dalam rangka pelaksanaan Misi Negara.

I.4. Manfaat Pedoman Pengamanan Informasi

1. Pedoman dalam melakukan kajian risiko terkait penggunaan TI dan melakukan tata kelola keamanan informasi secara efektif, efisien, dan konsisten sesuai hasil kajian risiko;
2. Pedoman dalam melakukan penilaian mandiri (self-assesment) secara objektif dengan menggunakan Indeks Keamanan Informasi (Indeks KAMI);
3. Pedoman dalam menyusun sistem dokumentasi minimum yang diperlukan untuk menerapkan tata kelola keamanan informasi;

I.5. Lokasi

Kegiatan Penyelenggaraam Persandian dan Keamanan Informasi Daerah Tahun 2018 berlokasi di Kabupaten Pesisir Selatan.

I.6. Organisasi

Untuk kelancaran pekerjaan, kegiatan ini dilaksanakan sesuai dengan struktur organisasi yang telah dibakukan dan akan melibatkan bidang-bidang terkait yang ada pada Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan.

I.7. Waktu Pelaksanaan

Kegiatan Penyelenggaraam Persandian dan Keamanan Informasi Daerah Tahun 2018 dilaksanakan selama 12 bulan yaitu dari bulan Januari s/d Desember 2018.

I.8. Biaya

Sumber dana untuk mendukung Kegiatan Penyelenggaraam Persandian dan Keamanan Informasi Daerah Tahun 2018 dianggarkan dana sebesar Rp. 59.263.500,- (Lima puluh sembilan juta dua ratus enam puluh tiga ribu lima ratus rupiah) yang berasal dari APBD Kabupaten Pesisir Selatan Tahun Anggaran 2018 DPA Organisasi Perangkat Daerah Dinas Komunikasi dan Informatika Kabupaten Pesisir Selatan.

BAB II
DATA DAN ANALISIS PENGAMANAN DATA INFORMASI DI KABUPATEN PESISIR SELATAN

Pelaksanaan monitoring dan peninjauan serta pemeriksaan terhadap aplikasi dan system yang digunakan oleh Organisasi Prangkat Daerah yang berada di Kabupaten Pesisir Selatan dalam hal pengamanan data informasi yang berada di OPD masing-masing belum ada yang menerapkan system yang telah di standarkan oleh Badan Siber dan Sandi Negara, dari seluruh OPD yang telah dilakukan analisis dapat direkap dan dinilai bobot nilai dari keseluruhannya berdasarkan kelompok criteria, diantaranya sebagai berikut:

1. Sekretariat Daerah ;
2. Sekretariat DPRD;
3. Inspektorat ;
4. Dinas Pendidikan dan Kebudayaan;
5. Dinas Kesehatan;
6. Dinas Pemberdayaan Masyarakat dan Desa, Pengendalian Penduduk dan Keluarga Berencana;
7. Dinas Penanaman Modal Pelayanan Perizinan Terpadu Satu Pintu;
8. Dinas Kependudukan dan Pencatatan Sipil;
9. Dinas Sosial, Pemberdayaan Perempuan dan Perlindungan Anak;
10. Dinas Tanaman Pangan, Hortikultura dan Perkebunan;
11. Dinas Pariwisata, Pemuda dan Olahraga;
12. Dinas Perikanan;
13. Dinas Pekerjaan Umum dan Penataan Ruang;
14. Dinas Perhubungan;
15. Dinas Koperasi, UMKM, Perdagangan dan Perindustrian;
16. Dinas Perumahan Rakyat, Kawasan Permukiman dan Pertanahan;
17. Dinas Pengelola Sumber Daya Air;
18. Dinas Peternakan dan Kesehatan Hewan;
19. Satuan Polisi Pamong Praja dan Pemadam Kebakaran;
20. Dinas Pangan;
21. Dinas Komunikasi dan Informatika;
22. Dinas Lingkungan Hidup;
23. Dinas Kearsipan dan Perpustakaan;
24. Dinas Tenaga Kerja dan Transmigrasi.
25. Badan Perencanaan Daerah, Penelitian dan Pengembangan;
26. Badan Pengelola Keuangan Daerah;
27. Badan Kepegawaian dan Pengembangan Sumber Daya Manusia;
28. Badan Pendapatan;
29. Badan Penanggulangan Bencana.
30. Rumah Sakit Umum Daerah Dr. M. Zein Painan.
31. Kecamatan Koto XI Tarusan;
32. Kecamatan Bayang;
33. Kecamatan Bayang Utara;
34. Kecamatan IV Jurai;

35. Kecamatan Batang Kapas;
36. Kecamatan Sutera;
37. Kecamatan Lengayang;
38. Kecamatan Ranah Pesisir;
39. Kecamatan Linggo Sari Baganti;
40. Kecamatan Air Pura;
41. Kecamatan Pancung Soal;
42. Kecamatan Ranah Ampek Hulu Tapan;
43. Kecamatan Basa Ampek Balai Tapan;
44. Kecamatan Lunang; dan
45. Kecamatan Silaut.

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**
I	**Karakteristik Instansi**	
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	C
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	C
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus	C
1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	C
1,6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	C
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	C
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak	C

1,9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih [C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih	C
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)	C
	Skor penetapan Kategori Sistem Elektronik	**10**

Bagian II: Tata Kelola Keamanan Informasi				
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
Fungsi/Instansi Keamanan Informasi				
2,1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Tidak Dilakukan
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Tidak Dilakukan
2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2,4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2,5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2,7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan
2,8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Tidak Dilakukan

2.11	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Tidak Dilakukan
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Tidak Dilakukan
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Tidak Dilakukan
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Tidak Dilakukan
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Tidak Dilakukan
2.17	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak Dilakukan
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan
2.20	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	Tidak Dilakukan
2.21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak Dilakukan
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan
			Total Nilai Evaluasi Tata Kelola	**0**

Bagian III: Pengelolaan Risiko Keamanan Informasi

Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
		Kajian Risiko Keamanan Informasi		
3,1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan
3,2	II	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Tidak Dilakukan
3,3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan
3,4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?	Tidak Dilakukan
3,5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Tidak Dilakukan
3,6	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Tidak Dilakukan
3,7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Tidak Dilakukan
3,8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Tidak Dilakukan
3,9	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Tidak Dilakukan
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Tidak Dilakukan
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Tidak Dilakukan
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak Dilakukan
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Tidak Dilakukan

3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	0

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi				
4,1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Tidak Dilakukan
4,2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Tidak Dilakukan
4,3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Tidak Dilakukan
4,4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Tidak Dilakukan
4,5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?	Tidak Dilakukan
4,6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Tidak Dilakukan
4,7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan
4,8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Tidak Dilakukan
4,9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?	Tidak Dilakukan
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan
4,11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Tidak Dilakukan

4,12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Tidak Dilakukan
4,13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Tidak Dilakukan
4,14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Tidak Dilakukan
4,15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Tidak Dilakukan
4,16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan
4.17	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak Dilakukan
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Tidak Dilakukan
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan
Pengelolaan Strategi dan Program Keamanan Informasi				
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Tidak Dilakukan
4,21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Tidak Dilakukan
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Tidak Dilakukan
4,23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Tidak Dilakukan
4,24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Tidak Dilakukan
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan
4,26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan

4,27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan
4,28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak Dilakukan
4,29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan
			Total Nilai Evaluasi Kerangka Kerja	0

Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
Pengelolaan Aset Informasi				
5,1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Tidak Dilakukan
5,2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan
5,3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Tidak Dilakukan
5,4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	Tidak Dilakukan
5,5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Tidak Dilakukan
5,6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Tidak Dilakukan
5,7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Tidak Dilakukan
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5,8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda	Tidak Dilakukan
5,9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak Dilakukan
5.10	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak Dilakukan
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	Tidak Dilakukan

5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak Dilakukan
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Tidak Dilakukan
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak Dilakukan
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak Dilakukan
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Tidak Dilakukan
5.18	II	1	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	Tidak Dilakukan
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Tidak Dilakukan
5.20	III	2	Proses pengecekan latar belakang SDM	Tidak Dilakukan
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Tidak Dilakukan
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Tidak Dilakukan
5.23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Tidak Dilakukan
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Tidak Dilakukan
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan
5.27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan
Pengamanan Fisik				
5.28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Tidak Dilakukan
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Tidak Dilakukan
5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Tidak Dilakukan
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Tidak Dilakukan
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Tidak Dilakukan
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	Tidak Dilakukan

5.34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Tidak Dilakukan
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Tidak Dilakukan
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Tidak Dilakukan
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera.	Tidak Dilakukan
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Tidak Dilakukan
			Total Nilai Evaluasi Pengelolaan Aset	0

Bagian VI: Teknologi dan Keamanan Informasi				
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	
Pengamanan Teknologi				
6,1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Tidak Dilakukan
6,2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Tidak Dilakukan
6,3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Tidak Dilakukan
6,4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Tidak Dilakukan
6,5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Tidak Dilakukan
6,6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Tidak Dilakukan
6,7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Tidak Dilakukan
6,8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Tidak Dilakukan
6,9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Tidak Dilakukan

6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Tidak Dilakukan
6.11	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak Dilakukan
6.12	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan
6.13	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Tidak Dilakukan
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Tidak Dilakukan
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Tidak Dilakukan
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Tidak Dilakukan
6.17	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Tidak Dilakukan
6.18	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Tidak Dilakukan
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Tidak Dilakukan
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Tidak Dilakukan
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak Dilakukan
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Tidak Dilakukan
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?	Tidak Dilakukan
6.25	III	3	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Tidak Dilakukan
6.26	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	0

Indeks KAMI (Keamanan Informasi)

Responden:
Satuan KerjaDirektoratDepartemen

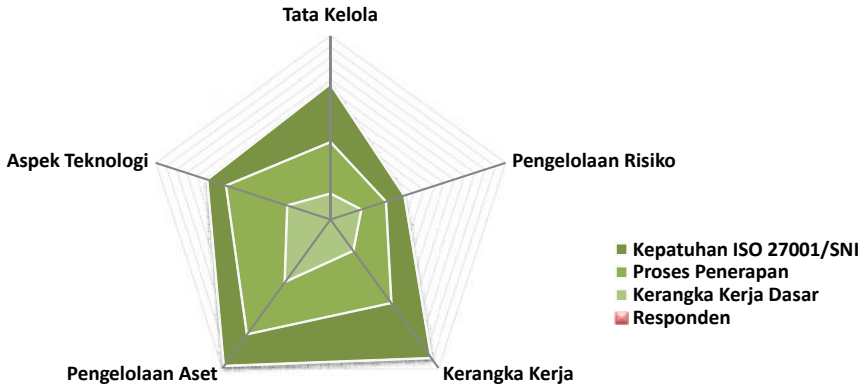
Alamat 1Alamat 2Kota Kode Pos

(Kode Area) Nomor Telpon
user@departemen_responden.go.id
HH/BB/TTTT

Hasil Evaluasi Akhir: **Tidak Layak**

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori 0

Skor Kategori SE	: 10	Kategori SE		**Rendah**
Tata Kelola	: 0	Tk Kematangan:	**I**	
Pengelolaan Risiko	: 0	Tk Kematangan:	**I**	**I**
Kerangka Kerja Keamanan Informasi	: 0	Tk Kematangan:	**I**	**s/d**
Pengelolaan Aset	: 0	Tk Kematangan:	**I**	**I**
Teknologi dan Keamanan Informasi	: 0	Tk Kematangan:	**I**	



BAB III

REALISASI KEUANGAN

Pelaksanaan sosialisasi Perundang-undangan ini dianggarkan sebesar Rp. 59.263.500,- dengan realisasi kegiatan fisik tercapai 100%, dan anggaran terealisasi Rp. 55.684.800-, atau sebesar 93,96 %. Dari anggaran yang direncanakan tersebut tersisa sebesar Rp. 3.578.700 -. Untuk lebih jelasnya dapat dilihat pada table berikut ini.

No.	Jenis Belanja	Jumlah Anggaran	Realisasi Anggaran	Sisa Anggaran	%
		59.263.500	**55.684.800**	**3.578.700**	**93,96**
2	Belanja alat tulis kantor	2.671.000	2.366.000	305.000	**88,58**
3	Belanja perangko, materai dan benda pos lainnya	180.000	180.000	-	**100,00**
4	Belanja Bahan Bakar Minyak/Gas dan pelumas	5.737.500	4.877.400	860.100	**85,01**
5	Belanja cetak	1.425.000	1.425.000	-	**100,00**
6	Belanja sewa Sarana Mobilitas Darat	6.000.000	5.700.000	300.000	**95,00**
7	Belanja makanan dan minuman pelatihan	1.100.000	-	1.100.000	**-**
8	Belanja perjalanan dinas dalam daerah	15.600.000	15.500.000	100.000	**99,36**
9	Belanja perjalanan dinas luar daerah Dalam Propinsi	10.950.000	10.555.000	395.000	**96,39**
10	Belanja perjalanan dinas luar daerah Luar Propinsi	15.600.000	15.081.400	518.600	**96,68**

BAB IV

TOLOK UKUR KINERJA

Tolak Ukur Kinerja merupakan capaian income dan outcome dari sebuah kegiatan yang dilaksanakan. Pada Kegiatan Pembangunan dan Pengembangan Program Aplikasi Elektronik pada Tahun 2018 ini realisasi hasilnya melebihi dari target yang ditetapkan, Untuk lebih jelasnya dapat dilihat pada tabel berikut ini.

Indikator		Target	Realisasi
Capaian : Program	Terselenggaranya pengamanan informasi dan data plikasi Perangkat Daerah	100%	100%
Masukan :	Jumlah Dana Yang Dibutuhkan	Rp. 59.263.500,-	Rp. 55.684.800-, (93,96 %)
Keluaran :	Terlaksananya monitoring dan pemantauan serta pengamanan informasi dan data plikasi Perangkat Daerah	45 OPD	45 OPD
Hasil :	Tersdedianya buku pedoman pengamanan informasi dan data plikasi Perangkat Daerah	3 Buku Pedoman Pengamanan data dan informasi	3 Buku Pedoman Pengamanan data dan informasi

BAB V
PENUTUP

Laporan Akhir Hasil Kegiatan Penyelenggaraan Persandian dan Keamanan Informasi Daerah Tahun 2018 ini disusun ini dibuat sebagai salah satu dokumentasi dari sebuah kegiatan yang berisikan rencana, proses dan hasil kegiatan selama satu tahun anggaran.

4.1. Kesimpulan

Kegiatan Penyelenggaraan Persandian dan Keamanan Informasi Daerah Tahun 2018 pada Dinas Komunikasi dan Informasi Kabupaten Pesisir Selatan yang bentuk pekerjaannya berupa monitoring dan pemantauan data informasi OPD serta pembuatan buku pedoman pengamanan data informasi dapat berjalan lancar, yang dapat dimanfaatkan dan dipedomani untuk kedepannya dalam mengamankan data dain informasi masing-masing OPD.

4.2. Saran

1. Penyelenggaraan E-Government di Kabupaten Pesisir Selatan masih sangat membutuhkan pedoman dan keahlian dalam mengamankan data dan informasi di setiap OPD.
2. Buku pedoman pengamanan data dan informasi ini, diharapkan dapat digunakan dan dipedomani oleh setiap OPD dalam mengamankan data dan informasinya masing-masing.