LAPORAN
DEKSTOP ASSESMENT
INDEKS KAMI

Instansi/Perusahaan: Pemerintah Provinsi Kepulauan Riau	**Narasumber Instansi/Perusahaan:** 1. Donny Firmansyah, ST. 2. Edi Wansyah, S.Tr.
Unit Kerja: Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau	
Alamat: Komplek Pusat Pemerintahan Provinsi Kepulauan Riau – Istana Kota Piring, Gedung Sultan Mahmud Riayat Syah (Gedung B2 Lantai III) Pulau Dompak	**Tel:** 0771-4575023
Email: kominfo@kepriprov.go.id	**Pimpinan Unit Kerja:** Drs. Zulhendri, M.Si.

A. **Ruang Lingkup**:

1. Instansi / Unit Kerja:

   Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau

2. Fungsi Kerja:
   Dalam melaksanakan tugasnya, Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau menyelenggarakan fungsi sebagai berikut :
   1. Perumusan kebijakan di bidang pengelolaan dan layanan informasi publik, pengelolaan komunikasi publik, teknologi informasi dan komunikasi serta layanan e-government;
   2. Pelaksanaan kebijakan di bidang pengelolaan dan layanan informasi publik, pengelolaan komunikasi publik, teknologi informasi dan komunikasi serta layanan e-government;
   3. Pelaksanaan evaluasi dan pelaporan di bidang pengelolaan dan layanan informasi publik, pengelolaan komunikasi publik, teknologi informasi dan komunikasi serta layanan e-government;
   4. Pelaksanaan administrasi dinas;
   5. Pengelolaan kegiatan kesekretariatan, meliputi perencanaan dan evaluasi, keuangan, umum dan kepegawaian;
   6. Pelaksanaan fungsi lain yang diberikan oleh gubernur.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor	Komplek Pusat Pemerintahan Provinsi Kepulauan Riau – Istana Kota Piring, Gedung Sultan Mahmud Riayat Syah (Gedung B2 Lantai III) Pulau Dompak
2	Data Center	Komplek Pusat Pemerintahan Provinsi Kepulauan Riau – Istana Kota Piring, Gedung Sultan Mahmud

		Riayat Syah (Gedung B2 Lantai III) Pulau Dompak
3	Disaster Recovery Center	Belum ada

B. **Nama /Jenis Layanan Publik**:

Layanan yang masuk ruang lingkup adalah Sistem Layanan Infrastruktur (Data Center, Aplikasi, Jaringan, Server) Sistem Informasi dan Sistem Komunikasi yang dikelola oleh Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau.

C. **Aset TI yang kritikal**:

1. Informasi:
   - Data Pegawai

2. Aplikasi:
   - SIMANJA
   - SIAP Kepri
   - PPID
   - SILAT

3. Server:
   Kepri Cyber System (KCS)

4. Infrastruktur Jaringan/Network:
   - Internet

D. DATA CENTER (DC):

ADA, dalam ruangan khusus

E. DISASTER RECOVERY CENTER (DRC):

BELUM ADA

Status Ketersediaan Dokumen Kerangka Kerja
Sistem Manajemen Keamanan Informasi (SMKI)

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

No	Nama Kebijakan	Cakupan Dokumen	Ada/Tidak
1	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain: • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan kontrol	Ada

		• Struktur dan metodologi manajemen risiko • Organisasi dan tanggungjawab keamanan informasi	
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggungjawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah	Ada
3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara intenal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.	Tidak
4	Kebijakan Manajemen Risiko TIK	Berisi metodologi / ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.	Ada
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana/k darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.	Ada
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).	Ada

No	Nama Prosedur/ Pedoman	Cakupan Dokumen	Ada/Tidak
1	Pengendalian Dokumen	Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan jika tidak digunakan, daftar dan pengendalian dokumen eksternal yang menjadi rujukan	Ada
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi	Ada

3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor	Tidak
4	Tindakan Perbaikan & Pencegahan	Berisi tatacara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TI	Ada
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/daya “rahasia” baik softcopy maupun hardcopy, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada Instansi	Ada
6	Pengelolaan Removable Media & Disposal Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (tape/hard disk/Flashdisk/CD) dan penghapusan informasi ataupun penghancuran media	Ada
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Berisi proses monitoring penggunaan CPU, storage, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil monitoring	Ada
8	User Access Management	Berisi proses dan tatacara pendaftaran, penghapusan dan review hak akses user, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, database, internet, email dan internet)	Ada
9	Teleworking	Pengendalian dan pengamanan penggunaan hak akses secara remote (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.	Tidak
10	Pengendalian instalasi software & Hak Kekayaan Intelektual	Berisi daftar software standar yang diijinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan software yang tidak diijinkan	Ada
11	Pengelolaan Perubahan (Change Management) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/database/versi dari aset TIK yang mengalami perubahan.	Ada
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan/pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.	Ada

Dokumen yang diperiksa:

1. Peraturan Gubernur Nomor 50 Tahun 2017 Tentang Pelaksanaan dan Pengembangan E-Government Provinsi Kepulauan Riau
2. Dokumen RFC 2350 Pemprov Kepri
3. Keputusan Gubernur Kepulauan Riau Nomor 996.a Tahun 2018 Tentang Pejabat Pengelola Teknologi Informasi/*Chief Information Officer* di Provinsi Kepulauan Riau
4. Peraturan Gubernur Kepulauan Riau Nomor 33 Tahun 2017 Tentang Standarisasi Penyelenggaraan Portal dan Situs Web di Lingkungan Pemerintah Provinsi Kepulauan Riau
5. Keputusan Gubernur Kepulauan Riau Nomor 1218 Tahun 2019 Tentang Computer Security Incident Response Team Provinsi Kepulauan Riau (KepriProv-CSIRT)

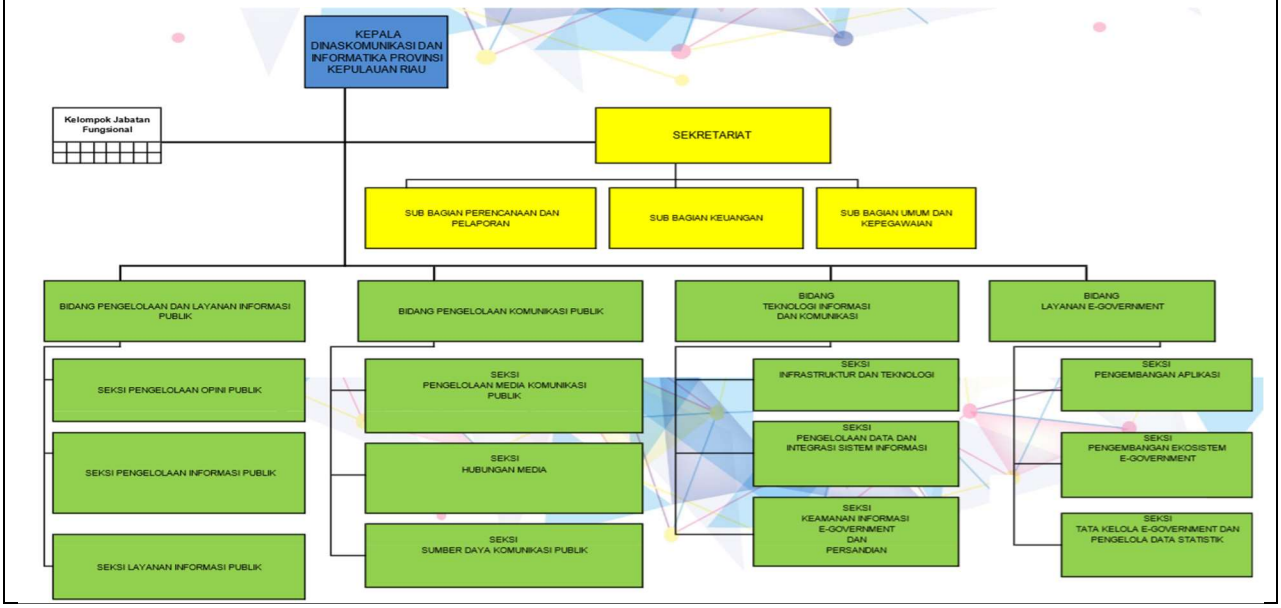
6. Keputusan Kepala Dinas Kominfo Provinsi Kepulauan Riau Tentang Tim Teknis Percepatan Pelaksanaan E-Government Provinsi Kepulauan Riau
7. Keputusan Gubernur Kepulauan Riau Nomor 83 Tahun 2017 Tentang Tim Percepatan Pelaksanaan E-Government Provinsi Kepulauan Riau
8. Daftar Inventarisasi Aplikasi di Lingkungan Pemerintah Provinsi Kepulauan Riau
9. Dokumen Inventaris Server di Data Center
10. Kartu Inventaris Barang
11. Dokumen Topologi Jaringan Pemprov Kepri
12. Dokumen Daftar Informasi Admin/Penanggungjawab Aplikasi dan Website, Klasifikasi Kritikalitas dan Dampak Kerugian dari Insiden Keamanan Informasi Pemerintah Provinsi Kepulauan Riau Tahun 2019
13. Laporan Penanganan Insiden Keamanan Informasi pada Website di URL : http://kominfo.kepriprov.go.id dan http://kesbangpol.kepriprov.go.id/
14. Laporan Penanganan Insiden dispora.kepriprov.go.id
15. Dokumen Panduan Pelaporan Insiden
16. Dokumen Panduan Penanganan DdoS, Malware, SQL Injection, Web Defacement dan Phishing
17. SOP Network Operation Center (NOC)
18. SOP Pemanfaatan Cadangan (Backup) Data Aplikasi
19. SOP Pemantauan Website
20. SOP Pembaruan Data Contact Person
21. SOP Pembuatan Layanan Domain, Web Hosting, VPS dan Colocation Server
22. SOP Penanggulangan Keamanan Sistem Informasi
23. SOP Pengelolaan Website
24. SOP Penitipan dan Pengembalian Server
25. Dokumen Laporan Keterangan Pertanggungjawaban (LKPJ) Tahun 2020
26. Peraturan Gubernur Kepulauan Riau Tentang Tata Kerja Pengelola Layanan Informasi dan Dokumentasi di Lingkungan Pemerintah Provinsi Kepulauan Riau
27. Dokumen Rancangan Peraturan Gubernur Kepulauan Riau Tentang Sistem Manajemen Keamanan Informasi
28. Dokumen Perjanjian Kerjasama Antara Dinas Komunikasi dan Informatika Kepulauan Riau dan Balai Sertifikasi Elektronik Lembaga Sandi Negara
29. Dokumen Tabel Hasil Evaluasi Jabatan Struktural Di Lingkungan Pemerintah Provinsi Kepulauan Riau
30. Laporan Audit Keamanan Aplikasi Simanja Provinsi Kepulauan Riau serta Report Acunetix
31. Dokumen Report Acunetix untuk bkpsdm.kepriprov.go.id
32. Laporan Hasil Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian Pemda Provinsi Kepulauan Riau Tahun 2020
33. Peraturan Gubernur Kepulauan Riau Nomor 59 Tahun 2017 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Perangkat Daerah
34. Peraturan Gubernur Kepulauan Riau Nomor 16 Tahun 2021 Tentang Penyelenggaraan Sertifikat Elektronik Di Lingkungan Pemerintah Provinsi Kepulauan Riau
35. Dokumen Rencana Strategis Tahun 2021-2026 Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau
36. Dokumen Risk Register
37. Dokumen Rincian Perubahan Belanja Sub Kegiatan Satuan Kerja Perangkat Daerah
38. Laporan IT Security Assessment Pemprov Kepri
39. Peraturan Gubernur Kepulauan Riau Nomor 61 Tahun 2017 Tentang Jadwal Retensi Arsip Pemerintah Provinsi Kepulauan Riau
40. Undangan Sosialisasi Indeks Keamanan Informasi (KAMI) Tahun 2021
41. Dokumen Surat Pesanan Pekerjaan : Belanja Sewa Bandwidth 800 Mbps (November-Desember)
42. Dokumen Perjanjian Kerahasiaan (Non Disclosure Agreement) Antara Dinas Kominfo Provinsi Kepri dengan Tenaga Pendukung Web Programmer Senior Dalam Hal Pekerjaan sebagai Tenaga Pendukung Web Programmer Senior pada Diskominfo Provinsi Kepri

43. Dokumen Notulen Bimtek dan Sosialisasi Implementasi Tanda Tangan Digital di Diskominfo Pemprov Kepri
44. Laporan Pengelolaan Portal Keamanan Informasi Website CSIRT
45. Dokumen Undangan Sosialisasi Sertifikat Elektronik oleh Badan Siber dan Sandi Negara untuk Pejabat di Lingkungan Pemprov Kepulauan Riau
46. Laporan Pencadangan (Backup) Data Sistem Informasi Manajemen Kinerja Periode Desember 2021
47. Laporan Pencadangan (Backup) Data Akun Cpanel Pada Web Host Manager Periode Desember 2021
48. Laporan Pejabat Pengelola Informasi dan Dokumentasi Tahun 2019
49. Laporan Pejabat Pengelola Informasi dan Dokumentasi Tahun 2020
50. Peraturan Gubernur Kepulauan Riau Nomor 76 Tahun 2017 Tentang Tata Kerja Pengelola Layanan Informasi dan Dokumentasi di Lingkungan Pemprov Kepri
51. Draft SOP Pencadangan (Backup) Data
52. Draft SOP Pemulihan (Recovery) Data
53. Dokumen Formulir Catatan Wawancara Pelamar
54. Tangkapan Layar NAS
55. Laporan Pelaksanaan Tandatangan Elektronik di Pemprov Kepri
56. Surat Pernyataan Perjanjian Kerahasian (Non Disclosure Agreement) dalam rangka IT Security Assessment
57. Peraturan Daerah Provinsi Kepulauan Riau Nomor 3 Tahun 2016 Tentang Penyelenggaraan Kearsipan Provinsi Kepulauan Riau
58. Foto Ruangan dan Akses Data Center
59. SOP Pengembangan Aplikasi
60. SOP Penghancuran Data
61. Dokumen Surat Edaran Perihal Penguatan Keamanan Informasi pada aplikasi SIMANJA
62. File log dan tangkapan Layar Clock, daftar antivirus server, server time dan antivirus dekstop Smadav

Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber instansi/lembaga disimpulkan sbb:

I. KONDISI UMUM:

1. Struktur organisasi satuan kerja dalam ruang lingkup berada di bawah Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau sebagai berikut

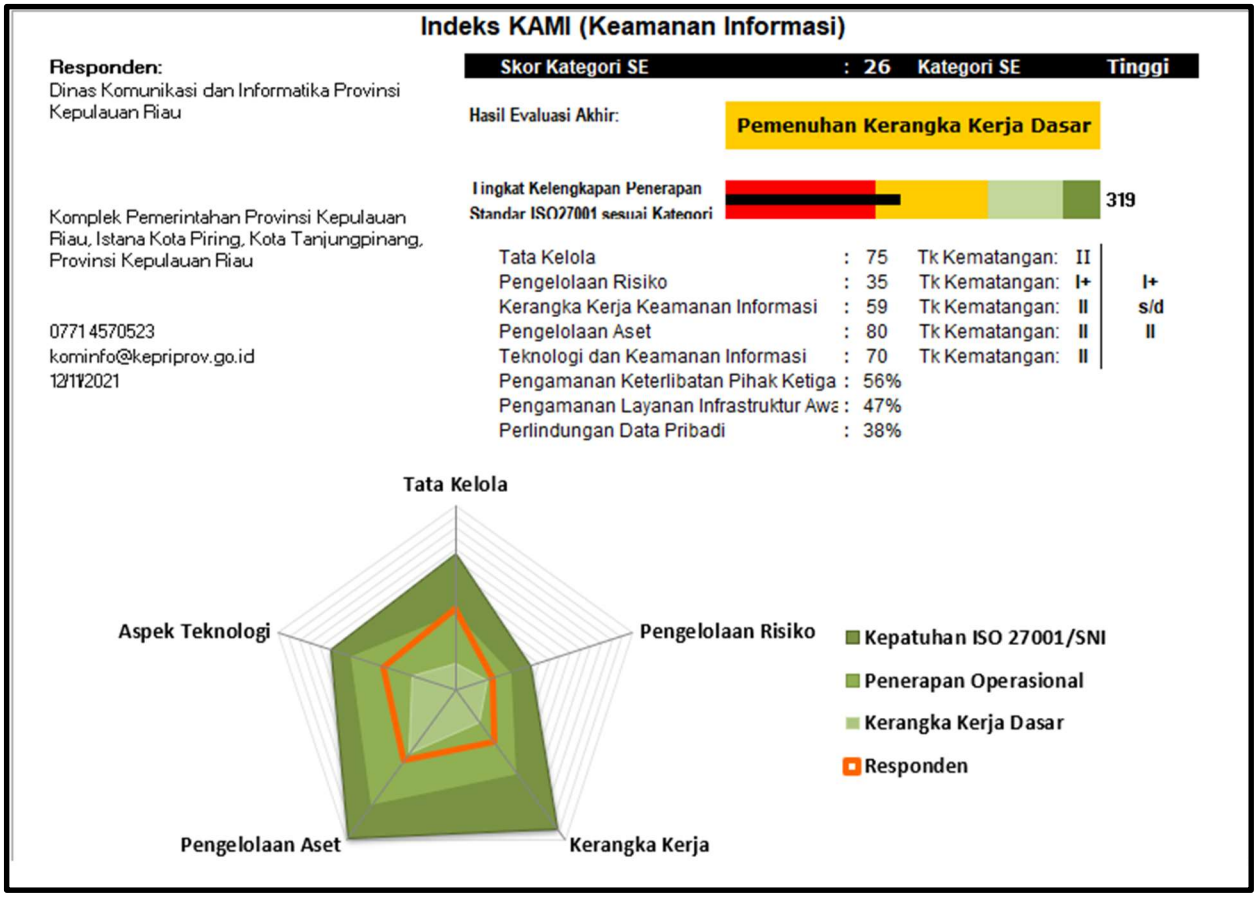


2. SDM pengelola terdiri dari:

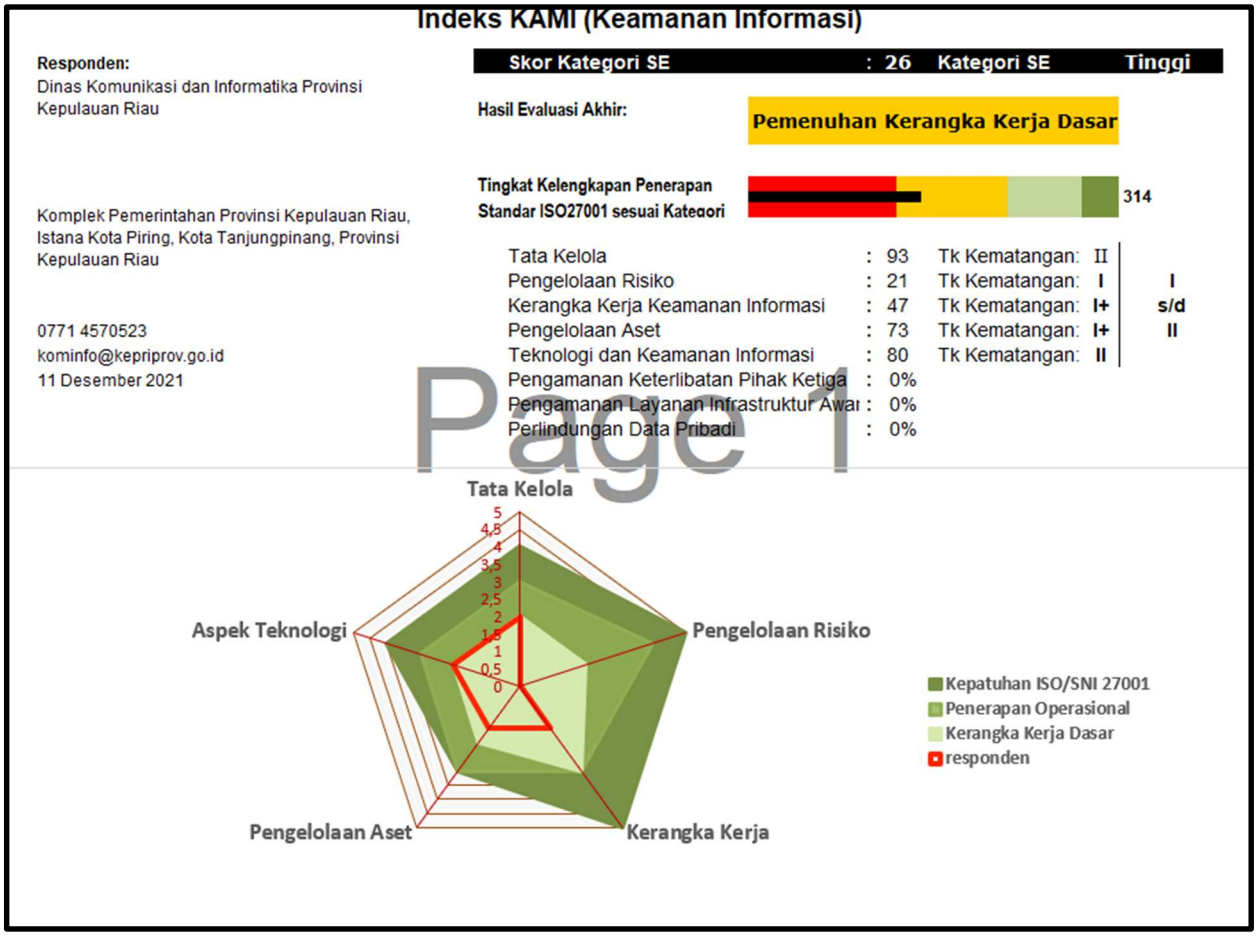
   Jumlah pegawai di Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau adalah 37 orang PNS, 10 orang PTT, 59 orang THL dan 8 orang Tenaga Ahli.

3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Total Score Sebelum Verifikasi: 319



Total Score Setelah Verifikasi: 314



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Pimpinan dari Diskominfo Provinsi Kepri sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen yang tertuang dalam Renstra Dinas Komunikasi dan Informatika Tahun 2021-2026.
2. Diskominfo Provinsi Kepri telah memiliki fungsi yang tugas dan tanggung jawabnya mengelola keamanan informasi serta penanggungjawab pelaksanaan pengamanan informasi memiliki wewenang yang sesuai dan diberikan alokasi sumber daya yang sesuai, berdasarkan Rencana SMKI, Peraturan Gubernur Nomor 59 Tahun 2017 dan Renstra Diskominfo Provinsi Kepri Tahun 2021-2026.
3. Diskominfo Provinsi Kepri telah mendefinisikan standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi.
4. Diskominfo Provinsi Kepri telah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi kepada semua pihak yang terkait, contoh kegiatan yaitu bimbingan teknis mengenai indeks kami.
5. Penanggungjawab pengelolaan keamanan informasi telah melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi secara rutin dan resmi.
6. Pimpinan instansi sudah mempertimbangkan kondisi dan permasalahan keamanan informasi di instansi dalam pengambilan keputusannya.
7. Pimpinan instansi telah menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi.
8. Diskominfo Provinsi Kepri telah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya.

9. Diskominfo Provinsi Kepri telah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu pelaksananya.

B. Kelemahan/Kekurangan
1. Diskominfo Provinsi Kepri belum melakukan identifikasi data pribadi yang digunakan dalam proses kerja dan belum menerapkan pengamanan terhadap data tersebut sesuai dengan peraturan perundangan yang berlaku.
2. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) belum didefinisikan dan dialokasikan.
3. Diskominfo Provinsi Kepri belum melakukan identifikasi legislasi, perangkat hukum dan standar lainnya yang terkait keamanan informasi yang harus dipatuhi dan juga belum melakukan analisa tingkat kepatuhannya.
4. Diskominfo Provinsi Kepri belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

III. ASPEK RISIKO:

A. Kekuatan/Kematangan
1. Diskominfo Provinsi Kepri telah memiliki rancangan SMKI.
2. Diskominfo Provinsi Kepri telah mendefinisikan kepemilikan dan pihak pengelola (custodian) untuk beberapa aset informasi termasuk aset utama yang dimiliki beserta dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset tersebut.
3. Diskominfo Provinsi Kepri telah menyusun langkah mitigasi dan penanggulangan risiko bagi aset aplikasi dan sistem yaitu berupa panduan pelaporan insiden dan panduan penanganan insiden (DDOS, Malware, SQL Injection, Web Defacement dan Phishing).

B. Kelemahan/Kekurangan
1. Diskominfo Provinsi Kepri belum memiliki program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
2. Diskominfo Provinsi Kepri belum menetapkan penanggungjawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan.
3. Kerangka kerja pengelolaan risiko keamanan informasi belum terdokumentasi, belum secara resmi digunakan.
4. Kerangka kerja pengelolaan risiko belum mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dampak kerugian terhadap instansi dan belum menetapkan ambang batas tingkat risiko yang dapat diterima.
5. Diskominfo Provinsi Kepri belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
6. Langkah mitigasi dan penanggulangan risiko belum disusun sesuai dengan tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya.
7. Belum ada pemantauan secara berkala terhadap status penyelesaian langkah mitigasi risiko dan belum ada evaluasi terhadap penyelesaian langkah mitigasi
8. Kerangka kerja pengelolaan risiko belum secara berkala dikaji.

IV. ASPEK KERANGKA KERJA:

A. Kekuatan/Kematangan
1. Diskominfo Provinsi Kepri telah menerapkan proses (mencakup pelaksana, mekanisme, jadwal, materi dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi kepada semua pihak terkait termasuk pihak ketiga**.**
2. Diskominfo Provinsi Kepri telah memiliki dokumen untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi, yaitu berupa SOP penanggulangan keamanan informasi dan panduan pelaporan insiden.

3. Konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan.
4. Telah mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten.

B. Kelemahan/Kekurangan
1. Kebijakan keamanan informasi belum ditetapkan secara formal dan belum dipublikasikan kepada seluruh karyawan/pihak terkait.
2. Belum ada mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
3. Kebijakan dan prosedur keamanan informasi yang ada belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi.
4. Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK belum tercantum dalam kontrak dengan pihak ketiga.
5. Belum adanya konsekuensi dari pelanggaran kebijakan keamanan informasi yang didefinisikan, dikomunikasikan dan ditegakkan.
6. Diskominfo Provinsi Kepri belum menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya.
7. Diskominfo Provinsi Kepri belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
8. Belum menerapkan proses pengembangan sistem yang aman (*secure* SDLC).
9. Belum tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) dan perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) serta belum dilakukan evaluasi terhadap hal tersebut.
10. Belum dilakukan evaluasi terhadap kebijakan dan prosedur keamanan informasi yang dimiliki.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan
1. Diskominfo Provinsi Kepri telah memiliki ketetapan terkait pertukaran data dengan pihak eksternal dan pengamannya.
2. Diskominfo Provinsi Kepri melakukan proses pengecekan latar belakang SDM.
3. Diskominfo Provinsi Kepri telah menerapkan proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
4. Diskominfo Provinsi Kepri sudah menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik, serta infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan gangguan pasokan listrik atau dampak dari petir.
5. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sudah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan sudah dilengkapi dengan fasilitas pendukung yang sesuai.

B. Kelemahan/Kekurangan
1. Belum adanya pendefinisian terkait klasifikasi aset informasi beserta tingkatan akses dari setiap klasifikasi aset informasi.
2. Belum tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset dan keperluan pengamanannya.
3. Belum tersedia proses pengelolaan perubahan dan proses pengelolaan konfigurasi terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten.

4. Belum tersedia proses untuk merilis suatu aset baru kedalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
5. Diskominfo Provinsi Kepri belum memiliki tata tertib penggunaan komputer, email, internet dan intranet, tata tertib pengamanan da penggunaan aset instansi terkait HAKI, peraturan terkait instalasi piranti lunak di aset TI milik instansi, peraturan yang mengatur terkait penggunaan data pribadi dan ketentuan terkait pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
6. Belum ada proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
7. Diskominfo Provinsi Kepri belum memiliki prosedur penghancuran data/aset yang sudah tidak diperlukan.
8. Belum ada prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
9. Belum tersedia daftar data/informasi yang harus di back-up dan laporan analisa kepatuhan terhadap prosedur backup.
10. Belum tersedia peraturan pengamanan perangkat komputasi milik instansi apabila digunakan diluar lokasi kerja resmi.
11. Belum ada mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
12. Belum 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.

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan
1. Diskominfo Provinsi Kepri sudah menerapkan segmentasi jaringan komunikasi sesuai dengan kepentingan.
2. Jaringan, sistem dan aplikasi yang digunakan sudah secara rutin dilakukan pemindaian.
3. Diskominfo Provinsi Kepri sudah memiliki rancangan redundan dan dilakukan monitoring untuk memastikan ketersediaan kapasitas yang cukup untuk keseluruhan infrastruktur jaringan, sistem dan aplikasi sesuai kebutuhan/persyaratan yang ada.
4. Setiap perubahan dalam sistem informasi dan upaya akses oleh yang tidak berhak sudah secar otomatis terekam di dalam log.
5. Diskominfo Provinsi Kepri sudah menerapkan enkripsi pada aset informasi penting sesuai kebijakan pengelolaan yang ada.
6. Diskominfo Provinsi Kepri sudah menerapkan pengamanan untuk mengelola kunci enkripsi yang digunakan.
7. Diskominfo Provinsi Kepri sudah menerapkan pengamanan untuk mendeteksi dan mecegah penggunaan akses jaringan yang tidak resmi.

B. Kelemahan/Kekurangan
1. Diskominfo Provinsi Kepri belum mempunyai standar dalam menggunakan enkripsi.
2. Seluruh sistem dan aplikasi belum secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
3. Laporan penyerangan virus/malware yang gagal/sukses belum ditindaklanjuti dan belum diselesaikan.

VIII. REKOMENDASI

1. Diskominfo Provinsi Kepri perlu melakukan identifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan terhadap data tersebut sesuai dengan peraturan perundangan yang berlaku. Identifikasi data pribadi dapat disusun sesuai dengan peraturan perundangan yang berlaku dengan merujuk pada Perkominfo Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik dan referensi hukum lainnya terkait dengan data pribadi.
2. Perlu menyusun dokumen *Business Continuity Plan* dan *Disaster Recovery Plan* (DRP).
3. Diskominfo Provinsi Kepri perlu melakukan identifikasi legislasi, perangkat hukum dan standar lainnya yang terkait keamanan informasi yang harus dipatuhi dan juga belum melakukan analisa tingkat kepatuhannya.
4. Diskominfo Provinsi Kepri perlu menyusun kebijakan/prosedur yang mendefinisikan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).
5. Diskominfo Provinsi Kepri perlu menyusun dan menganggarkan terkait program kerja pengelolaan risiko keamanan informasi.
6. Diskominfo Provinsi Kepri perlu menyusun kerangka kerja pengelolaan risiko keamanan informasi secara resmi dengan mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dampak kerugian terhadap instansi dan belum menetapkan ambang batas tingkat risiko yang dapat diterima. Kerangka kerja pengelolaan risiko belum secara berkala dikaji.
7. Perlunya menyusun pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporannya.
8. Dalam kerangka kerja pengelolaan risiko, perlu adanya pembagian peran dan tanggungjawab sampai dengan eskalasi pelaporan status pengelolaan risiko yang perlu diimplementasikan melalui hasil evaluasi pelaporan status pengelolaan risiko dan disampaikan kepada pimpinan secara periodik.
9. Diskominfo Provinsi Kepri perlu melaksanakan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
10. Dalam penyusunan langkah mitigasi dan penanggulangan risiko perlu disusun sesuai dengan tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya.
11. Perlu dilakukan pemantauan secara berkala terhadap status penyelesaian langkah mitigasi risiko dan belum ada evaluasi terhadap penyelesaian langkah mitigasi.
12. Perlu membuat mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpannya yang berupa SOP pengelolaan dokumen.
13. Diskominfo Provinsi Kepri perlu mencantumkan aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK dalam kontrak dengan pihak ketiga.
14. Dalam kebijakan SMKI perlu dicantumkan konsekwensi dari pelanggaran kebijakan keamanan informasi, dikomunikasikan dan ditegakkan baik di internal maupun eksternal Diskominfo Provinsi Kepri.
15. Menyusun kebijakan dan prosedur operasional dapat berupa SOP pengelolaan patch untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, hingga memastikan pemasangan dan melaporkannya.
16. Diskominfo Provinsi Kepri perlu menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
17. Menyusun prosedur untuk menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi.

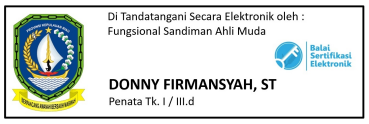
18. Diskominfo Provinsi Kepri perlu melakukan evaluasi kelayakan secara berkala pada seluruh kebijakan dan prosedur keamanan informasi.
19. Dalam pengelolaan aset, Diskominfo Provinsi Kepri perlu menuangkan definisi terkait klasifikasi aset informasi beserta tingkatan akses dari setiap klasifikasi aset informasi dalam peraturan.
20. Menyusun prosedur mengenai evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset dan keperluan pengamanannya.
21. Menyusun prosedur pengelolaan perubahan dan proses pengelolaan konfigurasi terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) dan menerapkan secara konsisten.
22. Menyusun prosedur rilis aplikasi yang perlu dituangkan dalam SOP manajemen rilis aplikasi dengan tujuan untuk menyediakan aplikasi yang sesuai dengan spesifikasi tingkat akurasi yang telah ditetapkan dan menjamin *quality assurance* teradap aplikasi yang akan naik ke *production*.
23. Diskominfo Provinsi Kepri perlu menyusun tata tertib penggunaan komputer, email, internet dan intranet, tata tertib pengamanan da penggunaan aset instansi terkait HAKI, peraturan terkait instalasi piranti lunak di aset TI milik instansi, peraturan yang mengatur terkait penggunaan data pribadi dan ketentuan terkait pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
24. Menyusun prosedur terkait penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi serta pelaporan insiden tersebut kepada pihak eksternal ataupun pihak yang berwajib.
25. Menyusun prosedur penghancuran data/aset yang sudah tidak diperlukan.
26. Menyusun prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
27. Perlu menyusun daftar data/informasi yang harus di back-up dan laporan analisa kepatuhan terhadap prosedur backup.
28. Perlu menyusun dan menetapkan peraturan pengamanan perangkat komputasi milik instansi apabila digunakan diluar lokasi kerja resmi.
29. Menerapkan mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
30. Menetapkan peraturan untuk pengamanan 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.
31. Diskominfo Provinsi Kepri perlu mencantumkan standar dalam menggunakan enkripsi (penerapan kriptografi) di kebijakan SMKI, serta membuat dokumen turunan dari kebijakan tersebut.
32. Seluruh sistem dan aplikasi perlu menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
33. Perlu menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelola keamanan informasi
34. Perlu menyusun laporan implementasi SMKI secara berkala dengan periode waktu tiap bulan dan disampaikan kepada pimpinan untuk dapat dilakukan evaluasi penerapan serta langkah perbaikan dalam menjaga terwujudnya keamanan informasi secara menyeluruh pada seluruh pemangku kepentingan.
35. Perlu meningkatkan kegiatan sosialisasi/literasi keamanan informasi menggunakan berbagai media baik offline maupun media sosial.
36. Perlu melakukan identifikasi kebijakan dan prosedur yang menjadi turunan kebijakan keamanan informasi dan melakukan sosialisasi secara kontinu dan berkelanjutan baik pihak internal maupun eksternal yang terkait dengan pengelolaan sistem elektronik.
37. Menyediakan proses (mencakup pelaksana, mekanisme, jadwal materi, dan salurannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.

38. Melakukan evaluasi kelayakan secara berkala pada seluruh kebijakan dan prosedur keamanan informasi.
39. Melakukan penjadwalan kegiatan audit internal terhadap kebijakan implementasi SMKI setelah ditetapkan kebijakan tersebut secara resmi sebagai salah satu bentuk kepatuhan terhadap penerapannya.

Jakarta, 29 Desember 2021

Dinas Komunikasi dan Informatika Provinsi Kepulauan Riau

1. Donny Firmansyah, S.T.



2. Edi Wansyah, S.Tr.

Assessor Indeks KAMI:

1.Assessor : Firman Maulana, S.E.

2. Assesor : Melita Irmasari, S.ST.,M.M.

3. Assesor : Ivan Bashofi, S.S.T.TP.

4. Assesor : Ni Putu Ayu Lhaksmi W.,S.Tr.TP.