GUBERNUR KALIMANTAN SELATAN

PERATURAN GUBERNUR KALIMANTAN SELATAN
NOMOR 078 TAHUN 2022

TENTANG

PEDOMAN MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR KALIMANTAN SELATAN,

Menimbang : bahwa untuk melaksanakan ketentuan pasal 11 ayat (3) Peraturan Daerah Provinsi Kalimantan Selatan Nomor 01 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, terkait pentingnya tersusunnya kebijakan keamanan informasi perlu menetapkan Peraturan Gubernur tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik.

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
5. Undang-Undang Nomor 8 Tahun 2022 tentang Provinsi Kalimantan Selatan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 68, Tambahan Lembaran Negara Republik Indonesia Nomor 6779);
6. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Perubahan atas Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 187, Tambahan Lembaran Negara Republik Indonesia Nomor 6402);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
10. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
12. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);

13. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
14. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang TIM Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488);
15. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
16. Peraturan Daerah Provinsi Kalimantan Selatan Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Kalimantan Selatan (Lembaran Daerah Provinsi Kalimantan Selatan Tahun 2016 Nomor 11, Tambahan Lembaran Daerah Provinsi Kalimantan Selatan Nomor 100);
17. Peraturan Daerah Provinsi Kalimantan Selatan Nomor 01 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Provinsi Kalimantan Selatan Tahun 2022 Nomor 1);
18. Peraturan Gubernur Kalimantan Selatan Nomor 095 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Perangkat Daerah Provinsi Kalimantan Selatan (Berita Daerah Provinsi Kalimantan Selatan Tahun 2019 Nomor 95) sebagaimana telah diubah beberapa kali, terakhir dengan Peraturan Gubernur Nomor 010 Tahun 2022 tentang Perubahan atas Peraturan Gubernur Kalimantan Selatan Nomor 095 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Perangkat Daerah Provinsi Kalimantan Selatan (Berita Daerah Provinsi Kalimantan Selatan Tahun 2022 Nomor 10);
19. Peraturan Gubernur Kalimantan Selatan Nomor 072 Tahun 2020 tentang Tugas, Fungsi dan Uraian Tugas Dinas Komunikasi dan Informatika Provinsi Kalimantan Selatan (Berita Daerah Provinsi Kalimantan Selatan Tahun 2016 Nomor 72);

MEMUTUSKAN:

Menetapkan: PERATURAN GUBERNUR TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Kalimantan Selatan.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Gubernur adalah Gubernur Provinsi Kalimantan Selatan.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Kalimantan Selatan.
5. Perangkat Daerah adalah unsur pembantu kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Dinas Komunikasi dan Informatika yang selanjutnya disebut Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang persandian, komunikasi, dan informatika.
7. Kepala Dinas adalah Dinas Komunikasi dan Informatika Provinsi Kalimantan Selatan.
8. Informasi adalah sebuah keterangan, pernyataan, gagasan, atau tanda-tanda yang mengandung nilai, makna dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, di dengar dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik.
9. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
10. Sistem Manajemen Keamanan Informasi yang selanjutnya disebut SMKI adalah bagian dari sistem manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan, dan memelihara keamanan informasi.
11. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
12. Sistem adalah kumpulan komponen atau elemen-elemen yang saling berhubungan satu sama lain untuk mencapai suatu tujuan tertentu.
13. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.

14. Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
15. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
16. Manajemen Kemanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE berkualitas.
17. Perangkat Keras adalah semua jenis piranti atau komponen komputer yang bagian fisiknya dapat dilihat secara kasat mata dan dirasakan langsung.
18. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait, dalam pengoperasian sistem Elektronik.
19. Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
20. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan atas informasi dan komunikasi secara Elektronik.
21. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan atas Informasi Elektronik.
22. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan atas informasi Elektronik.
23. Aplikasi SPBE adalah satu atau sekumpulan program computer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
24. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
25. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat Elektronik lainnya.
26. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengirimkan, dan/atau menyebarkan informasi Elektronik.
27. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media elektronik lainnya.
28. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik, telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman bagi Perangkat Daerah dalam mengelola pedoman manajemen Keamanan Informasi SPBE secara terpadu dalam memastikan terjaganya aspek kerahasiaan, keutuhan dan ketersediaan pada informasi.

(2) Proses manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:

a. penetapan ruang lingkup;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. standar operasional prosedur pengendalian;
f. manajemen risiko;
g. pengelolaan pihak ketiga;
h. evaluasi kinerja; dan
i. perbaikan berkelanjutan terhadap keamanan informasi.

BAB II
PENETAPAN RUANG LINGKUP

Pasal 3

(1) Penetapan ruang lingkup manajemen Keamanan Informasi SPBE meliputi:

a. data dan informasi SPBE;
b. aplikasi SPBE; dan
c. infrastruktur SPBE;

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Data dan informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf a merupakan data dan informasi dalam bentuk elektronik meliputi satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

(2) Aplikasi SPBE dan infrastruktur SPBE sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dan huruf c yang saling terintegrasi merupakan Sistem Elektronik.

BAB III
PENETAPAN PENANGGUNG JAWAB

Pasal 5

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam pasal 2 ayat (2) huruf b ditetapkan oleh Gubernur.

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.

(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi, Sekretaris Daerah disebut sebagai koordinator SPBE.

Pasal 6

(1) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:

a. ketua tim; dan

b. anggota tim.

(3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dapat dijabat oleh Kepala Dinas.

(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh Pimpinan Perangkat Daerah lainnya pada Pemerintah Daerah.

Pasal 7

(1) Ketua tim sebagaimana dimaksud dalam pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:

a. menetapkan standar operasional prosedur pengendalian Keamanan Informasi Pemerintah Daerah;

b. memastikan penerapan standar teknis dan prosedur pengendalian keamanan informasi di lingkungan Pemerintah Daerah;

c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;

d. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan

e. melaporkan pelaksanaan manajemen keamanan informasi dan penerapan standar teknis dan prosedur pengendalian keamanan informasi pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas:

a. mengoordinasikan dan/atau memastikan penerapan standar teknis dan prosedur pengendalian keamanan informasi pada Perangkat Daerah masing-masing.

b. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan

c. berkoordinasi dengan ketua tim terkait standar teknis dan prosedur pengendalian keamanan informasi dan standar teknis dan prosedur Keamanan SPBE.

BAB IV
PERENCANAAN

Pasal 8

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c ditetapkan oleh pelaksana teknis Keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:

a. program kerja Keamanan SPBE; dan

b. target realisasi program kerja Keamanan SPBE.

Pasal 9

(1) Program kerja Keamanan SPBE sebagaimana dimaksud pada pasal 8 ayat (2) huruf a paling sedikit meliputi:

a. edukasi kesadaran Keamanan SPBE;

b. penilaian kerentanan Keamanan SPBE;

c. peningkatan Keamanan SPBE;

d. penanganan insiden Keamanan SPBE; dan

e. audit Keamanan SPBE.

(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada pasal 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

BAB V
DUKUNGAN PENGOPERASIAN

Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan oleh koordinator SPBE.

(2) Koordinator SPBE memastikan pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi.

(3) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:

a. sumber daya manusia Keamanan SPBE;

b. teknologi keamanan SPBE; dan

c. anggaran keamanan SPBE.

Pasal 11

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada pasal 10 ayat (3) huruf a paling sedikit harus memiliki kompetensi:

a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan

b. keamanan aplikasi.

(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:

a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan

b. bimbingan teknis mengenai standar Keamanan SPBE.

(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan pengamanan informasi.

(4) Teknologi keamanan SPBE sebagaimana dimaksud pada pasal 10 ayat (3) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada ayat 10 ayat (3) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 12

(1) Standar dan prosedur pengendalian Keamanan Informasi sebagaimana dimaksud pada Pasal 2 ayat (2) huruf e ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.

(2) Standar dan prosedur pengendalian Keamanan SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan SMKI di lingkungan Pemerintah Daerah dengan persyaratan aspek meliputi:

a. keamanan perangkat teknologi informasi;

b. keamanan jaringan;

c. keamanan pusat data;

d. keamanan pembangunan dan pengembangan aplikasi SPBE;
e. keamanan sumber daya manusia;
f. pengelolaan aset;
g. perlindungan data pribadi;
h. kriptografi;
i. keamanan fisik dan lingkungan;
j. keamanan operasional;
k. keamanan komunikasi;
l. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
m. kebijakan terhadap pihak ketiga;
n. penanganan insiden Keamanan Informasi;
o. kelangsungan bisnis atau layanan TIK (*business continuity*);
p. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
q. audit internal Keamanan SPBE; dan/atau
r. kepatuhan Keamanan SPBE.

(3) Standar dan prosedur pengendalian Keamanan SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk surat edaran sekretaris daerah atau kebijakan teknis lainnya.

Pasal 13

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan standar dan prosedur pengendalian Keamanan SPBE sebagaimana dimaksud pada Pasal 12 ayat (2).

(2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman.

BAB VII
MANAJEMEN RISIKO

Pasal 14

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh setiap Perangkat Daerah untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE.

(2) Setiap Perangkat Daerah harus menerapkan prosedur pelaksanaan manajemen risiko meliputi:
a. komunikasi dan konsultasi;
b. Penetapan konteks risiko SPBE:
1. inventarisasi informasi umum

2. identifikasi sasaran SPBE;
3. penentuan struktur pelaksana Manajemen Risiko SPBE;
4. identifikasi pemangku kepentingan;
5. identifikasi peraturan perundang-undangan;
6. penetapan kategori risiko SPBE;
7. penetapan area dampak risiko SPBE;
8. penetapan kriteria risiko SPBE;
9. matriks analisis risiko SPBE dan level risiko SPBE;
10. selera risiko SPBE.

c. penilaian risiko SPBE:
   1. identifikasi risiko SPBE;
   2. analisis risiko SPBE; dan
   3. evaluasi risiko SPBE.

d. penanganan risiko SPBE:
   1. prioritas risiko;
   2. rencana penanganan risiko SPBE; dan
   3. risiko residual.

e. pemantauan dan reviu;

f. pencatatan dan pelaporan;

g. dokumen manajemen risiko SPBE:
   1. pakta integritas manajemen risiko SPBE;
   2. dokumen proses risiko SPBE; dan
   3. dokumen proses pengendalian risiko SPBE.

(3) Perangkat Daerah dalam melaksanakan penyusunan dokumen manajemen risiko di lingkungan kerjanya masing-masing dapat berkoordinasi kepada pelaksana teknis Keamanan Informasi.

BAB VIII
PENGELOLAAN PIHAK KETIGA

Pasal 15

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf g dilakukan oleh setiap Perangkat Daerah.

(2) Perangkat Daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.

(3) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.

(4) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian Sasaran Tingkat Layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

(5) Perangkat daerah dalam melaksanakan pengelolaan pihak ketiga di lingkungan kerjanya masing-masing dapat berkoordinasi kepada pelaksana teknis Keamanan Informasi.

BAB IX
EVALUASI KINERJA

Pasal 16

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf h dilakukan oleh koordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan keamanan SPBE.

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:

a. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan

b. mendukung dan merealisasikan program audit Keamanan SPBE.

(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

BAB X
PERBAIKAN BERKELANJUTAN

Pasal 17

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf i dilakukan oleh pelaksana teknis Keamanan SPBE.

(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:

a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;

b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan

c. tindak lanjut hasil audit Keamanan SPBE.

BAB XI
KETENTUAN PENUTUP

Pasal 18

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Kalimantan Selatan.

Ditetapkan di Banjarbaru
pada tanggal 1 Desember 2022

GUBERNUR KALIMANTAN SELATAN,

Ttd.

SAHBIRIN NOOR

Diundangkan di Banjarbaru
pada tanggal 1 Desember 2022

SEKRETARIS DAERAH PROVINSI
KALIMANTAN SELATAN,

Ttd.

ROY RIZALI ANWAR

BERITA DAERAH PROVINSI KALIMANTAN SELATAN
TAHUN 2022 NOMOR