GUBERNUR KALIMANTAN TIMUR

SALINAN

PERATURAN GUBERNUR KALIMANTAN TIMUR

NOMOR 54 TAHUN 2024

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR KALIMANTAN TIMUR,

Menimbang :

a. bahwa sesuai ketentuan Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Pasal 17 ayat (1) Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a perlu menetapkan Peraturan Gubernur tentang Sistem Manajemen Keamanan Informasi Pemerintah Daerah;

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 beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1 tambahan Lembaran Negara Republik Indonesia Nomor 6905);
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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);
5. Undang-Undang Nomor 10 Tahun 2022 tentang Provinsi Kalimantan Timur (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 70, Tambahan Lembaran Negara Republik Indonesia Nomor 6781);
6. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
8. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
9. 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);
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 Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
12. 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 261);

13. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
14. Peraturan Gubernur Kalimantan Timur Nomor 20 Tahun 2022 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah (Berita Daerah Provinsi Kalimantan Timur Tahun 2022 Nomor 20);
15. Peraturan Gubernur Kalimantan Timur Nomor 4 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah (Berita Daerah Provinsi Kalimantan Timur Tahun 2023 Nomor 4);

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Kalimantan Timur.
2. Gubernur adalah Gubernur Kalimantan Timur.
3. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom Provinsi Kalimantan Timur.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Kalimantan Timur.
5. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.

8. 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.
9. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
10. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan Keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
11. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
12. 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 integrase/penghubung, dan perangkat elektronik lainnya.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman sistem manajemen Keamanan Informasi di lingkungan Pemerintah Daerah.

(2) Penerapan sistem manajemen keamanan informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap aset informasi Pemerintah Daerah dari berbagai ancaman Keamanan Informasi.

(3) Sistem manajemen Keamanan Informasi di lingkungan Pemerintah Daerah sebagaimana dimaksud pada ayat (1), meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan terhadap Keamanan Informasi.

(4) Ketentuan lain dalam mendukung kebijakan keamanan internal SPBE sebagaimana dimaksud pada ayat (2) perlu menerapkan pengendalian teknis keamanan yang meliputi:
   a. manajemen resiko Keamanan SPBE;

b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
c. pengelolaan pihak ketiga.

BAB II
SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH

Pasal 3

(1) Penetapan ruang lingkup sistem manajemen Keamanan Informasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a meliputi:
a. data dan informasi;
b. pengelolaan Informasi; dan
c. kebijakan manajemen Keamanan Informasi.

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

Pasal 4

(1) Data dan Informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf a, merupakan data dan informasi dalam bentuk:
a. non elektronik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti kertas, papan tulis, spanduk, atau di dalam buku dan dokumen; dan/atau
b. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti database, pada file di dalam komputer, ditampilkan pada website, layar komputer, dan dikirimkan melalui jaringan telekomunikasi.

(2) Pengelolaan informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b meliputi:
a. Aplikasi SPBE; dan
b. Infrastruktur SPBE.

(3) Kebijakan manajemen Keamanan Informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf c meliputi penetapan prosedur pengendalian Keamanan Informasi Pemerintah Daerah.

(4) Penetapan prosedur pengendalian Keamanan Informasi Pemerintah Daerah sebagaimana dimaksud pada ayat (3) digunakan untuk mengimplementasikan manajemen Keamanan Informasi di lingkungan Pemerintah Daerah dengan cangkupan aspek meliputi:

a. keamanan perangkat TIK;
b. keamanan jaringan;
c. keamanan pusat data;
d. keamanan perangkat *end point*;
e. keamanan *remote working*;
f. keamanan penyimpanan elektronik;
g. pengelolaan akses kontrol;
h. pengendalian keamanan dari ancaman virus dan malware;
i. persayaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat IT *security;*
m. perlindungan data pribadi;
n. keamanan komunikasi;
o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
p. pengendalian Keamanan Informasi terhadap pihak ketiga;
q. penerapan kriptografi;
r. penanganan insiden Keamanan Informasi;
s. kelangsungan bisnis atau layanan TIK *(business continuity)*;
t. perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plans)*;
u. audit internal Keamanan SPBE; dan/atau
v. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.

(5) Penetapan prosedur pengendalian Keamanan Informasi sebagaimana dimaksud pada ayat (4) ditetapkan dengan Keputusan Gubernur.

Pasal 5

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (4) huruf c dilakukan oleh setiap perangkat daerah.

(2) PD 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) PD harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

(4) PD harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan Kerjasama dengan pihak ketiga.

(5) PD harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

Pasal 6

(1) Gubernur menetapkan penanggung jawab sistem manajemen Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b dengan Keputusan Gubernur.

(2) Penanggung jawab sistem manajemen Keamanan Informasi sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah Provinsi.

(3) Sekretaris Daerah sebagai penanggung jawab sebagaimana dimaksud pada ayat (2) merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 7

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen Keamanan Informasi Pemerintah Daerah, koordinator SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) menetapkan pelaksana teknis manajemen Keamanan Informasi Pemerintah Daerah.

(2) Pelaksana teknis manajemen Keamanan Informasi Pemerintah Daerah sebagai 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 pimpinan PD yang membidangi urusan komunikasi dan informatika.

(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri atas pimpinan PD atau pejabat administrator yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.

Pasal 8

(1) Ketua tim sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf a mempunyai tugas memastikan pelaksanaan manajemen Keamanan Informasi di lingkungan Pemerintah Daerah yang meliputi:
   a. memastikan penerapan standar teknis dan prosedur Keamanan Informasi;
   b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi; dan
   c. melaporkan pelaksanaan manajemen Keamanan Informasi pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf b mempunyai tugas:
   a. menerapkan standar teknis dan prosedur Keamanan Informasi pada PD masing-masing;
   b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur keamanan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
   c. memastikan keberlangsungan proses bisnis SPBE; dan
   d. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c ditetapkan oleh ketua tim pelaksana teknis Keamanan Informasi.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
   a. program kerja Keamanan Informasi yang disusun berdasarkan kategori risiko Keamanan Informasi; dan
   b. target realisasi program kerja Keamanan Informasi.

Pasal 10

(1) Program kerja Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a paling sedikit meliputi:
   a. edukasi kesadaran Keamanan Informasi;
   b. penilaian kerentanan keamanan Aplikasi SPBE dan Infrastruktur SPBE;
   c. peningkatan Keamanan Informasi;
   d. penanganan insiden Keamanan Informasi; dan
   e. audit Keamanan SPBE.

(2) Target realisasi program kerja Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya

Pasal 11

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf d dilakukan oleh koordinator SPBE.

(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
a. sumber daya manusia Keamanan Informasi;
b. teknologi Keamanan Informasi SPBE; dan
c. anggaran Keamanan Informasi.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen Keamanan Informasi diberikan alokasi sumber daya.

Pasal 12

(1) Sumber daya manusia Keamanan Informasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
a. keamanan infrastruktur TIK; dan
b. keamanan aplikasi.

(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus ad dukungan kegiatan:
a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur TIK dan keamanan aplikasi; dan/atau
b. bimbingan teknis mengenai standar Keamanan SPBE.

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

(4) Teknologi Keamanan Informasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b harus tersedia sesuai dengan kebutuhan dan tingkat urgensi dari setiap PD.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 13

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

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
b. menetapkan indikator kinerja pada setiap area proses;
c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
d. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan
e. 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.

Pasal 14

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f 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; dan/atau
b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB III
MANAJEMEN RESIKO KEAMANAN

Pasal 15

(1) Untuk mendukung manajemen Keamanan Informasi di lingkungan Pemerintah Daerah, setiap PD dapat menerapkan pengendalian teknis keamanan melalui manajemen risiko.

(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (risk register) dengan ketentuan subtansi meliputi:
a. inventarisasi aset elektronik dan non elektornik;
b. identifikasi ancaman dan kerentanan keamanan terhadap aset elektronik dan non elektornik;

c. penilaian risiko keamanan terhadap aset elektronik dan non elektornik;
d. penentuan prioritas risiko;
e. analisa dampak jika terjadi risiko;
f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan manajemen risiko mengacu sesuai dengan ketentuan peraturan perundang-undangan.

BAB IV
KETENTUAN PENUTUP

Pasal 16

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Samarinda
pada tanggal 30 Desember 2024

Pj. GUBERNUR KALIMANTAN TIMUR,

ttd

AKMAL MALIK

Diundangkan di Samarinda
pada tanggal 30 Desember 2024

SEKRETARIS DAERAH
PROVINSI KALIMANTAN TIMUR,

ttd

SRI WAHYUNI

BERITA DAERAH PROVINSI KALIMANTAN TIMUR TAHUN 2024 NOMOR 54.

Salinan sesuai dengan aslinya
SEKRETARIAT DAERAH PROV/KALTIM
KEPALA BIRO HUKUM,

SUPARMI
NIP. 19690512 198903 2 009