SALINAN

BUPATI LAMPUNG BARAT
PROVINSI LAMPUNG

PERATURAN BUPATI LAMPUNG BARAT
NOMOR 53 TAHUN 2025

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LAMPUNG BARAT,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di lingkungan Pemerintah Daerah Kabupaten Lampung Barat dari berbagai ancaman keamanan informasi baik dalam maupun luar, perlu melakukan pengelolaan manajemen keamanan informasi;

b. bahwa untuk memberikan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*), perlu dibentuk pedoman pelaksanaannya sebagaimana diatur dalam Pasal 3 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 Pemerintah Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi;

Mengingat : 1. Undang-Undang Nomor 6 Tahun 1991 tentang Pembentukan Kabupaten Daerah Tingkat II Lampung Barat (Lembaran Negara Republik Indonesia Tahun 1991 Nomor 64, Tambahan Lembaran Negara Republik Indonesia Nomor 3452);

2. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Repuplik Indonesia Tahun 2008 No 58, Tambahan Lembaran Negara Republik Negara Nomor 4843) sebagaimana telah diubah beberapa kali terakhir dengan Undang-undang Nomor 1 Tahun 2024 (Lembaran Negara Republik Indonesia Tahun 2024 Nomor I, Tambahan Lembaran Negara Republik Indonesia 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 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, (Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

5. 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 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 6856);

6. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);

7. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);

8. 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);

9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

10. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Infomasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

11. Peraturan Daerah Kabupaten Lampung Barat Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Dearah sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Daerah Kabupaten Lampung Barat Nomor 4 Tahun 2023 (Lembaran Daerah Kabupaten Lampung Barat Tahun 2023 Nomor 4);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah Otonom yang selanjutnya disebut Daerah adalah Kesatuan masyarakat hukum yang mempunyai batas-batas wilayah yang berwenang mengatur dan mengurus urusan pemerintahan dan kepentingan masyarakat setempat menurut prakarsa sendiri berdasarkan aspirasi masyarakat dalam sistem Negara Kesatuan Republik Indonesia.

2. Pemerintah Daerah dan Bupati sebagai unsur penyelenggara Pemerintah Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.

3. Bupati adalah Bupati Lampung Barat.

4. Wakil Bupati adalah Wakil Bupati Lampung Barat.

5. Sekretaris Daerah adalah Sekretaris Daerah Lampung Barat.

6. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam menyelenggarakan urusan pemerintahan yang menjadi kewenangan daerah.

7. Dinas Komunikasi dan Informatika adalah Dinas Komunikasi dan Informatika Kabupaten Lampung Barat.

8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan Teknologi Informasi dan komunikasi secara elektronik maupun non- elektronik.

9. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran Informasi, materi atau energi untuk mencapai suatu tujuan.

10. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses. mengumumkan, menganalisis, dan menyebarkan 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. Keamanan Informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas ketersediaan dari Informasi.

13. Penyimpanan Informasi adalah suatu proses menyimpan Informasi dengan menggunakan media elektronik.

14. Data Center atau Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti Sistem komunikasi data dan penyimpanan data.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.

(2) Kebijakan internal manajemen kemanan informasi SPBE sebagaimana dimaksud 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.

(3) Ketentuan lain untuk menukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis kemanan yang meliputi:
   a. manajemen risiko;
   b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
   c. pengelolaan pihak ketiga.

BAB II
MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Penetapan Ruang Lingkup

Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE meliputi ;
   a. data dan informasi SPBE;
   b. aplikasi SPBE;
   c. infrastuktur SPBE; dan
   d. kebijakan Penanganan Insiden.

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

Bagian Kedua
Penetapan Penanggung Jawab.

Pasal 4

(1) Penetapan penanggung jawab manajemen keamanan Informasi SPBE dilaksanakan oleh Bupati.

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

(3) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, Sekretaris Daerah disebut juga sebagai Koordinator SPBE.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan pelaksanaan teknis Keamanan SPBE.

(2) Pelaksanaan 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 pimpinan perangkat daerah yang membidangi urusan komunikasi dan informatika.

(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan perangkat daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan aplikasi SPBE dan/atau Insfrastuktur SPBE di lingkungan Pemerintah Daerah.

Pasal 6

(1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE Pemerintah Daerah yang meliputi;
a. menetapkan prosedur pengendalian keamanan informasi SPBE pemerintah Kabupaten Lampung Barat;
b. mengevaluasi penetapan prosedur pengendalian keamanan informasi SPBE Lampung Barat;
c. memastikan penerapan keamanan Aplikasi SPBE dan infrastuktur SPBE sesuai dengan standar teknis dan prosedur keamanan SPBE yang telah ditetapkan sesuai dengan peraturan dan perundang-undangan;
d. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan Anggaran keamanan SPBE;

e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans;* dan
f. melaporkan pelaksanaan manajemen kemanan informasi SPBE pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas;
a. mengkoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada perangkat daerah masing-masing.
b. memastikan penerapan keamanan aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.
c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan disaster recovery plans; dan
d. berkoordinasi dengan ketua tim terkait penerapan keamanan aplikasi SPBE dan Infrastruktur SPBE.

Bagian Ketiga
Perencanaan

Pasal 7

(1) Perencanaan dilakukan oleh ketua tim pelaksana teknis Keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
a. program kerja Keamanan SPBE yang disusun berdasarkan kategori resiko keamanan
b. target realisasi program kerja keamanan SPBE.

Bagian Keempat
Dukungan Pengoperasian

Pasal 9

(1) Dukungan Pengoperasian dilakukan oleh koordinator SPBE.

(2) Dukungan pengoperasian sebagaimana yang dimaksud ayat (1) dilakukan degan meningkatkan kapasitas terhadap;
a. sumber daya manusia keamanan SPBE;
b. teknologi keamanan SPBE; dan
c. anggaran keamana SPBE.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 10

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 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 adanya dukungan kegiatan:
   a. pelatihan dan/atau sertifikasi keamanan aplikasi dan TIK: dan/atau;
   b. bimbingan teknis mengenai standarteknis dan prosedur 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 keamanan SPBE.

(4) Teknologi keamanan informasi sebagaimana dimaksud pada pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan.

Bagian Kelima
Evaluasi Kinerja

Pasal 11

(1) Evaluasi kinerja sebagaimana dimaksud 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

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan;
   a. kesesuaian perencanaan SPBE;
   b. efektivitas pelaksanaan layanan SPBE;
   c. penerapan pengendalian keamanan sistem elektronik;
   d. pengelolaan risiko dan penanganan insiden;
   e. menganalisis efektifitas pelaksanaan Keamanan SPBE;
   f. mendukung dan merealisasikan program audit keamanan SPBE; atau
   g. capaian kinerja dan tingkat kematangan SPBE.

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

Bagian Keenam
Perbaikan Berkelanjutan

Pasal 12

(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
b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
c. tindak lanjut hasil audit Keamanan SPBE.

Bagian Ketujuh
Pengendalian Teknis Keamanan

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) dilakukan oleh setiap perangkat daerah.

(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (*risk register*) dengan ketentuan subtansi meliputi :
a. inventarisasi aset SPBE;
b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
c. penilaian risiko keamanan terhadap aset SPBE;
d. penentuan prioritas resiko;
e. analisa dampak jika terjadi risiko;
f. analisa kontrol keamanan yang diterapkan; dan/ atau
g. rekomendasi kontrol keamanan.

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

Pasal 14

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 2 ayat (3) huruf b ditetapkan oleh ketua tim pelaksana keamanan SPBE.

(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) di:
a. keamanan perangkat teknologi Informasi komunikasi;
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. persyaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
j. pengelolaan aset;
k. keamananmigrasi data;
l. konfigurasi perangkat *IT security*;
m. perlindungan data pribadi;
n. keamanan komunikasi;
o. keamanan dalam akuisisi, pengembangan dan pemeliharaan sistem informasi;
p. pengendalian keamanan informaasi terhadap pihak ketiga;
q. penerapan kriptografi;
r. penangan insiden keamanan informasi;
s. kelangsungan bisnis atau layanan TIK (*bussiness 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

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam Keputusan Bupati.

Pasal 15

(1) Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 14 ayat (3).

(2) Setiap perangkat daerah bertanggung jawab dalam memastikan kegiatan operasional teknologiinformasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 16

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) 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 memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga.

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

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

BAB III
KETENTUAN PENUTUP

Pasal 17

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar semua orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Lampung Barat.

Ditetapkan di Liwa
pada tanggal 29 Desember 2025

BUPATI LAMPUNG BARAT,

ttd.

PAROSIL MABSUS

Diundang di Liwa
pada tanggal 29 Desember 2025

SEKRETARIS DAERAH
KABUPATEN LAMPUNG BARAT,

ttd.

NUKMAN

BERITA DAERAH KABUPATEN LAMPUNG BARAT TAHUN 2026 NOMOR 53

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

SARJAK
NIP. 19761020 200501 1 008