SALINAN

BERITA DAERAH KABUPATEN LABUHANBATU
NOMOR 13 TAHUN 2024

BUPATI LABUHANBATU
PROVINSI SUMATERA UTARA

PERATURAN BUPATI LABUHANBATU
NOMOR 13 TAHUN 2024
TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM
PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LABUHANBATU,

Menimbang : a. bahwa berdasarkan ketentuan Pasal 60 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, setiap pimpinan instansi pusat mempunyai tugas melakukan koordinasi dan menetapkan kebijakan Sistem Pemerintahan Berbasis Elektronik;

b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Labuhanbatu dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan

mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;

c. bahwa untuk melaksanakan ketentuan pasal 23 tentang Peraturan Bupati tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, terkait pentingnya tersusunnya kebijakan manajemen keamanan informasi;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang 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 7 Drt Tahun 1956 tentang Pembentukan Daerah Otonom Kabupaten-Kabupaten Dalam Lingkungan Provinsi Sumatera Utara (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 1092);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (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);

4. 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);
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 9 Tahun 2015 tentang Perubahan Kedua Atas Undang- Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
6. Undang-Undang Nomor 8 Tahun 2023 tentang Provinsi Sumatera Utara (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 55, Tambahan Lembaran Negara Republik Indonesia Nomor 6864);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran negara 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 Manejemen 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 4 Tahun 2021 tentang Pedoman

Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita negara Republik Indonesia Tahun 2021 Nomor 541);

14. Peraturan Bupati Labuhanbatu Nomor 31 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Labuhanbatu (Berita Daerah Kabupaten Labuhanbatu Tahun 2023 Nomor 31);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Labuhanbatu.
2. Pemerintahan adalah adalah penyelenggaraan urusan pemerintah daerah oleh pemerintah daerah dan dewan perwakilan rakyat daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

3. Pemerintah Daerah adalah Bupati sebagai Perangkat Daerah adalah unsur Pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Bupati adalah Bupati Labuhanbatu.
5. Sekretaris Daerah adalah Sekretaris Daerah Labuhanbatu.
6. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
7. Sistem Pemerintahan Berbasis Elektronik atau yang selanjutnya disingkat dengan SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
8. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
9. Keamanan informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, serta terjaganya aspek kerahasiaan, keutuhan, dan ketersediaan dari informasi.
10. Keamanan SPBE mencakup aspek kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, infrastruktur SPBE, dan aplikasi SPBE.
11. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (confidentiality) atas informasi dan komunikasi secara elektronik.

12. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (integrity) atas informasi elektronik.
13. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (availability) atas informasi elektronik.
14. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
15. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan layanan SPBE.
16. 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 penghubung, dan perangkat elektronik lainnya.

BAB II
MAKSUD DAN TUJUAN

Pasal 2

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

(2) Kebijakan internal manajemen keamanan 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.

Pasal 3

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

BAB III
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam pasal 2 ayat (2) huruf a meliputi:
   a. data dan informasi SPBE;
   b. aplikasi SPBE; dan
   c. Infrastruktur SPBE.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset daerah yang harus diamankan dalam SPBE.

Pasal 4

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

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

(3) Sekretaris daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundangundangan.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 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 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 dan infrastruktur 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 di lingkungan Pemerintah Daerah yang meliputi:
a. menetapkan prosedur pengendalian keamanan

informasi SPBE Daerah;

b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di Lingkungan Pemerintah Daerah;
c. memastikan penerapan keamanan aplikasi SPBE dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
d. merumuskan, mengoordinasikan, 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 keamanan informasi SPBE pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas:

a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian;
b. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada Perangkat Daerah masing- masing;
c. memastikan penerapan keamanan aplikasi SPBE dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
d. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan

e. berkoordinasi dengan ketua tim terkait penerapan keamanan aplikasi SPBE dan infrastruktur SPBE.

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2ayat (2) huruf c ditetapkan oleh ketua tim 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 8

(1) Program kerja Keamanan SPBE sebagaimana dimaksud pada pasal 7 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 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

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

(2) 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.

(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 pada pasal 9 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
   a. keamanan 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 kompetensi keamanan aplikasi dan TIK; dan/atau
   b. bimbingan teknis mengenai standar teknis 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 pada pasal 9 ayat (2) huruf c disusun berdasarkan

perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang- undangan.

Pasal 11

(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. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
   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.

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.

BAB IV
PENGENDALIAN TEKNIS KEAMANAN

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam pasal 2 ayat (3) huruf a 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 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.

Pasal 14

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

digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah dengan cakupan aspek dapat meliputi:

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. persayaratan keamanan terkait pembangunan;
j. pengembangan aplikasi SPBE;
k. pengelolaan aset;
l. keamanan migrasi data;
m. konfigurasi perangkat *IT Security*;
n. perlindungan data pribadi;
o. keamanan komunikasi;
p. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
q. pengendalian keamanan informasi terhadap pihak ketiga;
r. penerapan kriptografi;
s. penanganan insiden keamanan informasi;
t. kelangsungan bisnis atau layanan TIK (*business continuity*);
u. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
v. audit internal keamanan SPBE; dan/atau
w. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) selanjutnya ditetapkan dalam bentuk 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 teknologi informasi 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) huruf c 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 beserta kode sumbernya.
(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 V
KETENTUAN PENUTUP

Pasal 17

Pada saat mulai berlakunya Peraturan Bupati ini, maka Peraturan Bupati Labuhanbatu Nomor 28 Tahun 2018 tentang Sistem Manajemen Keamanan Informasi Pemerintah Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Labuhanbatu (Berita Daerah Kabupaten Labuhanbatu Tahun 2018 Nomor 28) dicabut dan dinyatakan tidak berlaku.

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Labuhanbatu

Ditetapkan di Rantauprapat
pada tanggal 19 September 2024

Plt. BUPATI LABUHANBATU,

ttd

ELLYA ROSA SIREGAR

Diundangkan dalam Berita Daerah
pada tanggal 19 September 2024

SEKRETARIS DAERAH
KABUPATEN LABUHANBATU,

ttd

HASAN HERI RAMBE

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM SETDAKAB

KHAIRUL FAHMI
PEMBINA TINGKAT I
NIP. 197103151997031005