GUBERNUR KEPULAUAN BANGKA BELITUNG

PERATURAN GUBERNUR KEPULAUAN BANGKA BELITUNG
NOMOR 15 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR PROVINSI KEPULAUAN BANGKA BELITUNG,

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Provinsi Kepulauan Bangka Belitung, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. 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 Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan Sistem Pemerintahan Berbasis Elektronik;

c. bahwa untuk melaksanakan ketentuan pasal 37 ayat 3 Peraturan Daerah Provinsi Kepulauan Bangka Belitung Nomor 6 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik, terkait pentingnya tersusunnya kebijakan manajemen keamanan informasi dalam rangka mendukung pencapaian penerapan SPBE yang efektiv, efisien dan berkesinambungan serta layanan SPBE yang berkualitas;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c perlu menetapkan Peraturan Gubernur Kepulauan Bangka Belitung 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 27 Tahun 2000 tentang Pembentukan Provinsi Kepulauan Bangka Belitung (Lembaran Negara Republik Indonesia Tahun 2000 Nnomor 21, Tambahan Lembaran Negara Republik Indonesia Nomor 4033);

3. 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 beberapa kali diubah terakhir dengan UndangUndang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842);

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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan 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. 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);

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 Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik;

10. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
11. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
12. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE;
13. Peraturan Daerah Nomor 6 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Provinsi Kepulauan Bangka Belitung Tahun 2022 Nomor 3 Seri E);

MEMUTUSKAN

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

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Provinsi adalah Provinsi Kepulauan Bangka Belitung.
2. Pemerintah Daerah adalah Gubernur dan Perangkat Daerah sebagai unsur penyelenggara pemerintahan daerah.
3. Gubernur adalah Gubernur Kepulauan Bangka Belitung
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Kepulauan Bangka Belitung.
5. Satuan Kerja Perangkat Daerah yang selanjutnya disingkat SKPD adalah Satuan Kerja Perangkat Daerah Pemerintah Provinsi Kepulauan Bangka Belitung yang terdiri dari Sekretariat Daerah, Sekretariat DPRD, Badan Perencanaan Pembangunan Daerah, Inspektorat, Satuan Polisi Pamong Praja, Dinas Daerah, Lembaga Teknis Daerah dan Lembaga Lain.
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. Aset informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi, dan dimanfaatkan secara efektif.

10. Keamanan SPBE mencakup penjaminan 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 tugas atau fungsi Layanan SPBE.

16. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan system, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman kebijakan internal manajemen keamanan informasi SPBE.
(2) Kebijakan internal 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.

(3) 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 II

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 Pemerintah Provinsi Kepulauan Bangka Belitung yang harus diamankan dalam SPBE.

Pasal 4

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Gubernur

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah Pemerintah Provinsi Kepulauan Bangka Belitung

(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi, Sekretaris Daerah membentuk Tim Keamanan Informasi yang ditetapkan melalui keputusan.

(4) Ketua Tim Keamanan Informasi sebagaimana dimaksud pada ayat (3) dijabat oleh Kepala Perangkat Daerah yang membidangi urusan Persandian dan Keamanan Informasi.

(5) Sekretaris Daerah Pemerintah Provinsi Kepulauan Bangka Belitung sebagai penanggung jawab merupakan bagian ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang- undangan.

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 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 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 Infrastruktur SPBE di lingkungan Pemerintah Provinsi Kepulauan Bangka Belitung.

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 Provinsi Kepulauan Bangka Belitung yang meliputi:
   a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Provinsi Kepulauan Bangka Belitung;

b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Provinsi Kepulauan Bangka Belitung;
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 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.

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (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 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 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 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 Provinsi Kepulauan Bangka Belitung .

(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 II

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;
c. keamanan terhadap aset SPBE;
d. penilaian risiko keamanan terhadap aset SPBE;
e. penentuan prioritas risiko;
f. analisa dampak jika terjadi risiko;
g. analisa kontrol keamanan yang bisa diterapkan; dan/atau
h. 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 Provinsi Kepulauan Bangka Belitung dengan cangkupan 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 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.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk keputusan [Gunernur/Wali Kota/Bupati] atau surat edaran sekretaris daerah atau kebijakan teknis lainnya.

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 III

KETENTUAN PENUTUP

Pasal 17

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Pemerintah Provinsi Kepulauan Bangka Belitung.

Ditetapkan di Pangkalpinang
pada tanggal 3 Juni 2024

Pj. GUBERNUR
KEPULAUAN BANGKA BELITUNG,

SAFRIZAL ZA

Diundangkan di Pangkalpinang
pada tanggal 3 Juni 2024

Pj. SEKRETARIS DAERAH
PROVINSI KEPULAUAN BANGKA BELITUNG,

FERY AFRIYANTO

BERITA DAERAH PROVINSI KEPULAUAN BANGKA BELITUNG TAHUN 2024
NOMOR 10 SERI E