

SALINAN

BUPATI BEKASI
PROVINSI JAWA BARAT

PERATURAN BUPATI BEKASI
NOMOR 55 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI KABUPATEN BEKASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BEKASI,

Menimbang : a. bahwa dalam rangka melaksanakan Ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, dalam rangka memberikan perlindungan aset informasi yang dimiliki oleh Pemerintah Daerah Kabupaten dari berbagai bentuk ancaman baik dari internal maupun eksternal dengan tujuan untuk menjamin kerahasiaan, keutuhan dan ketersediaan aset informasi;

b. bahwa dalam rangka menjabarkan sistem dalam perlindungan informasi sebagaimana dimaksud pada huruf a tersebut diatas, perlu diatur ketentuan mengenai Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b tersebut diatas, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Kabupaten Bekasi;

Mengingat : 1. Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Barat (Berita Negara Tahun 1950) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1968 tentang Pembentukan Kabupaten Purwakarta dan Kabupaten Subang dengan Mengubah Undang-Undang Nomor

14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);

2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881) 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 2022 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

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 Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 Informasi dan Transaksi Elektronik Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

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 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

6. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembarna Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);

7. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indoensia 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 6856);

8. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601) sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti UndangUndang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembar Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

9. Peraturan Pemerintahan Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indomesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

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

11. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);

12. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 157);

13. Peraturan Menteri Pendayagunaan Aparatur Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);

14. Peraturan Menteri Komunikasi dan Informatika Nomor 16 Tahun 2022 tentang Kebijakan Umum Penyelenggaraan Audit Teknologi Informasi dan Komunikasi (Berita Negara Republik Indonesia Tahun 2022 Nomor 1374);

15. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektonik (Berita Negara Republik Indonesia Tahun 2017 Nomor 907);

16. 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);

17. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488);

18. 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);

19. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);

20. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2024 Nomor 655);

21. Peraturan Daerah Kabupaten Bekasi Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Bekasi (Lembaran Daerah Kabupaten Bekasi Tahun 2016 Nomor 6) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Daerah Kabupaten Bekasi Nomor 2 Tahun 2024 tentang Perubahan Kedua Peraturan Daerah Kabupaten Bekasi Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Bekasi (Lembaran Daerah Kabupaten Bekasi 2024 Nomor 2);

22. Peraturan Bupati Bekasi Nomor 42 Tahun 2020 tentang Rencana Induk Sistem Pemerintahan Berbasis Elektronik Kabupaten Bekasi Tahun 2020-2025 (Berita Daerah Kabupaten Bekasi Tahun 2020 Nomor 42);

23. Peraturan Bupati Bekasi Nomor 2 Tahun 2023 tentang Sistem Pemerintahan Berbasis Elektronik di Kabupaten Bekasi (Berita Daerah Kabupaten Bekasi Tahun 2023 Nomor 2);

24. Peraturan Bupati Bekasi Nomor 30 Tahun 2023 tentang Kewenangan, Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi Informatika Persandian dan Statistik Kabupaten Bekasi (Berita Daerah Kabupaten Bekasi Tahun 2023 Nomor 90);

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 Kabupaten adalah Daerah Kabupaten Bekasi.
2. Pemerintah Daerah Kabupaten adalah Bupati Sebagai Unsur Penyelenggara Pemerintahan Daerah yang memimpin Pelaksanaan Urusan Pemerintahan yang menjadi kewenangan Daerah otonom.
3. Bupati adalah Bupati Bekasi.
4. Sekretaris Daerah adalah Sekretaris Daerah Pemerintah Kabupaten Bekasi.
5. Perangkat Daerah Kabupaten adalah Perangkat Daerah di Lingkungan Pemerintahan Daerah Kabupaten Bekasi.
6. Dinas adalah Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
7. Kepala Dinas adalah Kepala Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Bekasi.
8. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemprosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
10. 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.

11. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
12. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian *(confidentiality)* atas informasi dan komunikasi secara Elektronik.
13. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan *(integrity)* atas Informasi Elektronik.
14. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan *(availability)* atas Informasi Elektronik.
15. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
17. 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 *integrase*/penghubung, dan perangkat Elektronik lainnya.

BAB II
MAKSUD DAN TUJUAN
Pasal 2

Maksud disusunnya Peraturan Bupati ini adalah sebagai kebijakan internal manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Bekasi.

Pasal 3

Tujuan disusunnya Peraturan Bupati ini adalah :

a. Sebagai pedoman pengelolaan Sistem Manajemen Keamanan Informasi (SMKI) secara terpadu untuk memastikan terjaganya kerahasiaan *(confidentiality)*, keutuhan *(integrity)* dan ketersediaan *(availability).*

b. Pengelolaan SMKI sebagaimana dimaksud pada huruf a, meliputi infrastruktur komputer, jaringan, sistem informasi atau aplikasi dan sumber daya manusia.

BAB III

RUANG LINGKUP

Pasal 4

(1) Ruang lingkup Kebijakan Internal manajemen keamanan informasi SPBE meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan terhadap keamanan informasi.

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

BAB IV

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 5

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 ayat (1) 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 Kabupaten Bekasi yang harus diamankan dalam SPBE.

Pasal 6

(1) Penanggung jawab sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b, dijabat oleh Sekretaris Daerah.
(2) Sekretaris Daerah sebagaimana dimaksud pada ayat (1) juga melaksanakan tugas sebagai koordinator SPBE.
(3) Penanggung jawab sebagaimana dimaksud pada ayat (1), ditetapkan dengan Keputusan Bupati

Pasal 7

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 6 ayat (2) 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 Kepala Dinas.
(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b, terdiri dari seluruh pimpinan perangkat Daerah lainnya yang memiliki, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di Lingkungan Pemerintah Kabupaten Bekasi.
(5) Ketua tim sebagaimana dimaksud dalam ayat (3), mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di Lingkungan Pemerintah Kabupaten Bekasi yang meliputi:
    a. menetapkan prosedur pengendalian keamanan informasi SPBE di Pemerintah Kabupaten Bekasi;
    b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di Lingkungan Pemerintah Kabupaten Bekasi;
    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.

(6) Anggota tim sebagaimana dimaksud dalam ayat (4), 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 8

(1) Perencanaan sebagaimana dimaksud dalam Pasal 4 ayat (1) 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 9

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.

Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 4 ayat (1) 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.

Pasal 11

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada Pasal 10 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 10 ayat (2) huruf b, harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada Pasal 10 ayat (2) huruf c, disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 12

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf e, dilakukan oleh koordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1), dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di 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 13

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 4 ayat (1) 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 berkesinambungan; dan
   c. tindak lanjut hasil audit Keamanan SPBE.

(4) Untuk melaksanakan evaluasi kinerja ditunjuk oleh koordinator SPBE.

BAB V

PENGENDALIAN TEKNIS KEAMANAN

Pasal 14

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 4 ayat (2) 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 15

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 ayat (2) 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 Kabupaten Bekasi dengan cangkupan aspek meliputi :
a. Pengendalian Informasi Terdokumentasi;
b. Internal Audit;
c. Keamanan Komunikasi Internal dan Eksternal;
d. Tinjauan Manajemen;
e. Penanganan Ketidaksesuaian dan Perbaikan;
f. Kerjasama Dengan Supplier;
g. Penggunaan *Removable* Media;
h. Klasifikasi dan Pengelolaan Informasi;
i. Pengelolaan Perubahan;
j. Pengelolaan Penanganan, Tindakan, dan Pencegahan Insiden & Gangguan Keamanan Informasi;
k. Instalasi Perangkat Lunak;
l. Pengelolaan Akses Kontrol & Hak Akses;
m. Kesadaran Keamanan Informasi dan Komunikasi;
n. Pengelolaan Kapasitas;
o. Pelindungan Hak Kekayaan Intelektual dan Kepatuhan Regulasi;
p. Manajemen Kelangsungan Bisnis (BCM) dan Keamanan Informasi;
q. Pengelolaan Kriptografi;
r. *Backup dan Restore*;

s. Keamanan Pusat Data (DC) dan Pusat Pemulihan Data (DRC);
t. Kompetensi SDM untuk Keamanan Informasi;
u. Keamanan Jaringan;
v. Pemeliharaan Perangkat Data Center;
w. Keamanan Fisik;
x. Perlindungan Keamanan dari Ancaman *Malware*;
y. Keamanan dalam Pengembangan Aplikasi SPBE;
z. Keamanan Perangkat *End Point*;
aa. Keamanan *Remote Working*;
ab. Keamanan Penyimpanan Elektronik;
ac. Pengelolaan Aset / Data / Informasi;
ad. Keamanan Migrasi Data;
ae. Perlindungan Data Pribadi;
af. Pengendalian Keamanan Informasi Terhadap Pihak Ketiga dan Keamanan Informasi Untuk Hubungan Dengan Pemasok;
ag. Perencanaan Pemulihan Bencana (*Disaster Recovery Plan*) Terhadap Layanan TIK;
ah. Penilaian dan Pengelolaan Risiko Keamanan Informasi;
ai. *Outsourcing* Infrastruktur Teknologi Informasi dan Komunikasi.

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

Pasal 16

Setiap Perangkat Daerah melaksanakan kegiatan operasional teknologi informasi berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 17

(1) Pembangunan atau pengembangan Aplikasi dan Infrastruktur dilakukan oleh Perangkat Daerah atau pengelolaan oleh Pihak Ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
(2) Perangkat Daerah menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.
(3) Perangkat Daerah membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan/*Service Level Agreement* (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB VI

KETENTUAN PENUTUP

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 Bekasi.

Ditetapkan di : Cikarang Pusat
pada tanggal : 22 November 2024

Pj. BUPATI BEKASI

Ttd

DEDY SUPRIYADI

Diundangkan di : Cikarang Pusat
Pada tanggal : 22 November 2024

Pj. SEKRETARIS DAERAH KABUPATEN BEKASI

Ttd

JAOHARUL ALAM

BERITA DAERAH KABUPATEN BEKASI TAHUN 2024 NOMOR 55