BUPATI KUBU RAYA
PROVINSI KALIMANTAN BARAT

PERATURAN BUPATI KUBU RAYA
NOMOR 30 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN
PEMERINTAH KABUPATEN KUBU RAYA

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KUBU RAYA,

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintah secara elektronik yang aman di lingkungan Pemerintah Kabupaten Kubu Raya perlu melaksanakan keamanan informasi untuk memastikan kerahasian, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastuktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Kubu Raya dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajeman keamanan informasi sistem pemerintahan berbasis elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dengan huruf a, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintah Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kubu Raya;

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 35 Tahun 2007 tentang Pembentukan Kabupaten Kubu Raya di Provinsi Kalimantan Barat (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 101, Tambahan Lembaran Negara Republik lndonesia Nomor 4751);

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 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 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 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
7. 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);
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 Pelindungan 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 Manajemen 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 Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
14. Peraturan Daerah Kabupaten Kubu Raya Nomor 15 Tahun 2019 tentang Perubahan atas Peraturan Daerah Kabupaten Kubu Raya Nomor 6 Tahun 2016 Tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Kubu Raya Tahun 2019 Nomor 15, Tambahan Lembaran Daerah Kabupaten Kubu Raya Nomor 75);
15. Peraturan Bupati Kubu Raya Nomor 27 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik dalam Penyelenggaraan Pemerintahan Daerah (Berita Daerah Kabupaten Kubu Raya Tahun 2021 Nomor 27);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN KUBU RAYA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Kubu Raya.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Kabupaten Kubu Raya.
3. Bupati adalah Bupati Kubu Raya.
4. Perangkat Daerah adalah Perangkat Daerah di lingkungan Pemerintah Kabupaten Kubu Raya.
5. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah suatu sistem tata kelola pemerintahan yang memanfaatkan teknologi informasi secara menyeluruh dan terpadu dalam pelaksanaan administrasi pemerintahan dan penyelenggaraan pelayanan publik pada Pemerintah Daerah.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan dan pemindahan informasi antar media.
7. 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 informasi.
8. Keamanan SPBE adalah penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, infrastruktur SPBE dan aplikasi SPBE.
9. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan *(confidentiality)* atas informasi dan komunikasi secara elektronik.

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

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai kebijakan internal Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pasal 3

(1) 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 resiko;
    b. penetapan prosedur pengendalian Keamanan Informasi SPBE; dan
    c. pengelolaan pihak ketiga.
(3) Penetapan ruang lingkup Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) huruf a meliputi :
    a. data dan informasi SPBE;
    b. aplikasi SPBE; dan
    c. infrastruktur SPBE.
(4) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (3) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dilaksanakan oleh Bupati.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekertaris Daerah.
(3) Sekertaris Daerah sebagai penanggung jawab, tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan ketentuan 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 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 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 Pemerintah 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 ketentuan 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 countinuity* dan *distater 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 ketentuan 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 3 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 8

(1) Program kerja keamanan SPBE sebagaimana dimaksud dalam 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 ayat (1) ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 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.
(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 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 SPBE sebagaimana dimaksud dalam 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 dengan ketentuan peraturan perundang-undangan.

Pasal 11

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 ayat (1) 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 3 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
    c. tindak lanjut hasil audit keamanan SPBE.

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh setiap Perangkat Daerah untuk menjamin keberlangsungan SPBE dengan minimalkan dampak risiko dalam SPBE.
(2) Setiap Perangkat Daerah harus menerapkan prosedur pelaksanaan manajemen risiko meliputi:
    a. Komunikasi dan konsultasi;
    b. Penetapan konteks risiko SPBE;
        1. Inventarisasi informasi umum;
        2. Indentifikasi sasaran SPBE;
        3. Penentuan struktur pelaksanaan manajemen risiko SPBE;
        4. Identifikasi pemangku kepentingan;
        5. Identifikasi peraturan perundang-undangan.risiko SPBE;
        6. Penetapan kategori risiko SPBE;
        7. Penetapan area dampak risiko SPBE;
        8. Penetapan kriteria;
        9. Matriks analisis risiko SPBE dan level risiko SPBE; dan
        10. Selera risiko SPBE;
    c. Penilaian risiko SPBE;
        1. Prioritas risiko;
        2. Analisis risiko SPBE; dan
        3. Evaluasi risiko SPBE;
    d. Penanganan risiko SPBE;
    e. Pemantauan dan review;
    f. Pencatatan dan pelaporan;
    g. Dokumen manajemen risiko SPBE;
        1. Pakta integritas manajemen risiko SPBE;
        2. Dokumen proses risiko SPBE; dan
        3. Dokumen proses pengendalian risiko SPBE.
(3) Perangkat Daerah dalam melaksanakan penyusunan dokumen manajemen risiko di lingkungan kerjanya masing-masing dapat berkoordinasi dengan pelaksana teknis keamanan informasi.

Pasal 14

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 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 Daerah dengan cakupan aspek 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. persyaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat informasi dan teknologi *security*;
m. perlindungan data pribadi;
n. keamanan komunikasi;
o. keamanan dalam proses akusisi, 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 dengan Keputusan Bupati.

Pasal 15

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam 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 3 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 kerja sama dengan pihak ketiga.
(5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan 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 setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Kubu Raya.

Ditetapkan di Sungai Raya
pada tanggal 2 September 2024
PENJABAT BUPATI KUBU RAYA,

SYARIF KAMARUZAMAN

Diundangkan di Sungai Raya
pada tanggal...4...September. 2024
SEKRETARIS DAERAH KABUPATEN KUBU RAYA,

YUSRAN ANIZAM
BERITA DAERAH KABUPATEN KUBU RAYA TAHUN ...2024... NOMOR.....30.....