BUPATI SAMPANG
PROVINSI JAWA TIMUR
PERATURAN BUPATI SAMPANG

NOMOR 17 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI SAMPANG,

Menimbang :

a. bahwa dalam rangka penyelenggaraan sistem pemerintahan berbasis elektronik yang aman di lingkungan Pemerintah Kabupaten Sampang, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
b. bahwa untuk memberikan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi serta infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah kabupaten Sampang dari segala jenis gangguan keamanan dalam penyelenggaraan sistem pemerintahan berbasis elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik.

Mengingat :

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 59, Tambahan Lembaga Negara Republik Indonesia Nomor 4844) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024

Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

2. 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);
3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2009 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);
4. Undang-Undang Nomor 12 Tahun 2023 tentang Provinsi Jawa Timur (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 59, Tambahan Lembaran Negara Republik Indonesia Nomor 6868);
5. 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);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Presiden Nomor 82 tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
8. 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);
9. 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);
10. 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);
11. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488);
12. 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);

13. Peraturan Daerah Nomor 3 Tahun 2020 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Sampang Tahun 2020 Nomor 3), sebagaimana telah diubah dengan Peraturan Daerah Nomor 2 Tahun 2022 tentang Perubahan Atas Peraturan Daerah Nomor 3 Tahun 2020 Tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Sampang Tahun 2022 Nomor 02);
14. Peraturan Bupati Nomor 125 Tahun 2022 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Sampang (Berita Daerah Kabupaten Sampang Tahun 2022 Nomor 125);
15. Peraturan Bupati Nomor 41 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sampang Tahun 2023 Nomor 41).

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 Daerah Kabupaten Sampang.
2. Pemerintah Daerah adalah Pemerintahan Daerah Kabupaten Sampang.
3. Bupati adalah Bupati Sampang.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Sampang.
5. Perangkat Daerah adalah perangkat daerah Pemerintah Kabupaten Sampang.
6. Dinas Komunikasi dan Informatika adalah Perangkat Daerah yang membidangi urusan pemerintahan di bidang komunikasi informatika Kabupaten sampang.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat 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, pengelolaan dan penyampaian, atau pemindahan informasi antar sarana/media.
9. Perangkat lunak adalah istilah khusus untuk data yang diformat dan disimpan secara digital, termasuk program komputer, dokumentasinya, dan berbagai informasi yang bisa dibaca, dan ditulis oleh komputer.

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. Sistem Manajeman Keamanan Informasi, yang selanjutnya disingkat SMKI, adalah bagian dari sistem manajeman secara keseluruhan berdasarkan pendekatan risiko bisnis untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi.
12. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
13. insiden keamanan informasi adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik
14. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun nonelektronik.
15. bidang keamanan teknologi, informasi dan komunikasi adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya
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 sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrase/penghubung, dan perangkat elektronik lainnya.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai pedoman bagi perangkat daerah dalam menerapkan SMKI secara terpadu untuk memastikan terjaganya aspek kerahasian (*conffidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) terhadap penyelenggaraan pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Sampang.
(2) Pengelolaan SMKI sebagaimana dimaksud pada ayat (1) meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan.
(3) 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.

Pasal 3

(1) Penetapan ruang lingkup sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a dilakukan oleh setiap Kepala Dinas dan Bupati.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) dilakukan dengan mendefinisikan:
    a. isu internal keamanan informasi SPBE dalam organisasi; dan
    b. isu eksternal keamanan informasi SPBE.
(3) Isu internal keamanan informasi SPBE dalam organisasi sebagaimana dimaksud pada ayat (2) huruf a didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE.
(4) Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud pada ayat (3) paling sedikit meliputi:
    a. data dan informasi SPBE;
    b. Aplikasi SPBE;
    c. aset Infrastruktur SPBE; dan
    d. kebijakan keamanan informasi SPBE yang telah dimiliki.
(5) Isu eksternal keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) huruf b didefinisikan sesuai dengan ketentuan peraturan perundang-undangan

BAB II
PENANGGUNG JAWAB

Pasal 4

(1) Bupati menetapkan penanggung jawab manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh sekretaris Daerah.
(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, sekretaris Daerah mempunyai tugas sebagai koordinator SPBE.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan 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 dijabat oleh pimpinan perangkat daerah yang

melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi.

(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.

(5) Pelaksana teknis keamanan SPBE sebagaimana dimaksud ayat (2) ditetapkan dengan Keputusan Bupati.

Pasal 6

(1) Ketua Tim yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas:
   a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
   b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE;
   d. mengkoordinasikan, memantau dan menerima laporan pengelolaan insiden keamanan informasi.
   e. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Daerah.
   f. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*

(2) Anggota Tim yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas:
   a. menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;
   b. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
   c. memastikan keberlangsungan proses bisnis SPBE;
   d. berkoordinasi dengan pejabat yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada Perangkat Daerah terkait perumusan program kerja dan anggaran Keamanan SPBE.
   e. mengkoordinasikan, memantau dan mengelola insiden keamanan informasi di perangkat daerah masing-masing;
   f. mengirim laporan dan mendokumentasikan proses pengelolaan insiden keamanan informasi di perangkat daerah masing-masing; dan
   g. melaksanakan dan mengelola langkah-langkah untuk tetap menjaga keberlangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*;

Pasal 7

(1) Perencanaan penetapan ruang lingkup pedoman manajemen keamanan informasi SPBE dilakukan oleh pelaksana teknis Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
    a. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan
    b. target realisasi program kerja Keamanan SPBE.
(3) Program kerja Keamanan SPBE sebagaimana dimaksud pada 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.
(4) Kategori risiko Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.
(5) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah setiap tahunnya.

Pasal 8

(1) Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:
    a. sosialisasi; dan
    b. pelatihan.
(2) Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf b dilaksanakan paling sedikit melalui:
    a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
    b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
    c. mengukur tingkat risiko Keamanan SPBE
(3) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam ayat (2).
(4) Peningkatan Keamanan SPBE dilaksanakan paling sedikit melalui:
    a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
    b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE

Pasal 9 ....

Pasal 9

Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf d dilaksanakan paling sedikit melalui:

a. mengidentifikasi sumber serangan;
b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. mendokumentasi bukti insiden yang terjadi; dan
e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.

Pasal 10

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 11

(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; dan
    b. anggaran Keamanan SPBE.
(3) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit harus memiliki kompetensi:
    a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan
    b. keamanan aplikasi.
(4) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (3), paling sedikit melakukan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan
    b. bimbingan teknis mengenai standar Keamanan SPBE.
(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 12

(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 SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
    b. menetapkan indikator kinerja pada setiap area proses;

c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
d. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan
e. 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, yang kemudian dilaporkan kepada Bupati dan BSSN

Pasal 13

(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; dan
    b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB III
MANAJEMEN RISIKO

Pasal 14

(1) Manajemen risiko sebagaimana dimaksud dalam pasal 2 ayat (3) huruf a dilakukan oleh setiap perangkat daerah.
(2) Setiap Perangkat Daerah atau Unit kerja penyelenggara Teknologi Informasi wajib melakukan proses Manajemen Risiko.
(3) Proses Manajemen Risiko sebagaimana dimaksud pada ayat (1) meliputi:
    a. inventarisasi aset SPBE;
    b. identifikasi ancaman dan kerentanan keamanan
    c. 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.
(4) Prosedur pelaksanaan manajemen risiko mengacu sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam 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.
(3) Pengendalian keamanan informasi SPBE di lingkungan Pemerintah Daerah 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.

Pasal 16

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 15 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.

BAB IV
PIHAK KETIGA

Pasal 17

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh setiap Perangkat Daerah.
(2) Perangkat Daerah sebagaimana dimaksud pada ayat (1) harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga:

a. memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
b. memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

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

(4) 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
PENDANAAN

Pasal 18

Pendanaan penyelenggaraan Manajemen Kemanan Informasi SPBE bersumber pada:
a. Anggaran Pendapatan dan Belanja Daerah; dan
b. sumber pendanaan lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
KETENTUAN PENUTUP

Pasal 19

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di : Sampang
pada tanggal : 15 Maret 2024

Pj. BUPATI SAMPANG,

ttd

Rudi Arifiyanto

Diundangkan di : Sampang
pada tanggal : 15 Maret 2024

SEKRETARIS DAERAH KABUPATEN SAMPANG,

ttd

Yuliadi Setiyawan

BERITA DAERAH KABUPATEN SAMPANG TAHUN 2024 NOMOR : 17