



BUPATI PASER
PROVINSI KALIMANTAN TIMUR
PERATURAN BUPATI PASER
NOMOR 35 TAHUN 2025
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH
DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI PASER,

- Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Daerah Kabupaten Paser, 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 arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Daerah Kabupaten Paser dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi;
- c. 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, pemerintah daerah harus menerapkan keamanan sistem pemerintahan berbasis elektronik;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi Pemerintah Daerah.
- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Perpanjangan Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1953 Nomor 9 (Sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 72, Tambahan Lembaran Negara Republik Indonesia Nomor

- 1820) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 8 Tahun 1965 tentang Pembentukan Daerah Tingkat II Tanah Laut, Daerah Tingkat II Tapin, dan Daerah Tingkat II Tabalong Dengan Mengubah Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Perpanjangan Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 51, Tambahan Lembaran Negara Republik Indonesia Nomor 2756);
3. 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 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 6841);
 4. 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 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
 5. 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);
 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 Daerah Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
 8. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan 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 (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);

10. 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);
11. 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);
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);
14. Peraturan Bupati Paser Nomor 20 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah (Berita Daerah Kabupaten Paser Tahun 2022 Nomor 20);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Pasal 1

1. Daerah adalah Kabupaten Paser.
2. Bupati adalah Bupati Paser.
3. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Paser.
4. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom Kabupaten Paser.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
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. Insiden Keamanan Informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
11. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
12. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari Sistem Elektronik
13. Manajemen risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian dan penentuan prioritas risiko yang kemudian akan dikelola, dipantau dan dikontrol untuk mengurangi dampak dan/atau kemungkinan terjadinya risiko tersebut.
14. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan fungsi layanan SPBE.
15. 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 integrasi/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

- (1) Peraturan Bupati ini dimaksudkan sebagai pedoman dalam pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.
- (2) Peraturan Bupati ini bertujuan untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap aset informasi Pemerintah Daerah dari berbagai ancaman Keamanan Informasi.

Pasal 3

Manajemen keamanan informasi SPBE sebagaimana dimaksud pada Pasal 2 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.

BAB II SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 4

Dalam hal mendukung kebijakan keamanan informasi SPBE sebagaimana dimaksud pada Pasal 2 ayat (2) perlu menerapkan pengendalian teknis keamanan yang meliputi:

- a. manajemen risiko keamanan SPBE;
- b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
- c. pengelolaan pihak ketiga.

Pasal 5

- (1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf a meliputi:
 - a. data dan informasi SPBE;
 - b. aplikasi SPBE; dan
 - c. infrastruktur SPBE.
 - d. Kebijakan keamanan informasi SPBE yang telah dimiliki
- (2) Penetapan Ruang Lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.
- (3) Manajemen keamanan informasi SPBE ini berlaku untuk seluruh Perangkat Daerah di lingkungan Pemerintah Daerah.

Pasal 6

- (1) Data dan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a merupakan data dan informasi dalam bentuk :
 - a. non elektronik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti kertas, papan tulis, spanduk, atau di dalam buku dan dokumen; dan/atau
 - b. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti database, pada file di dalam komputer, ditampilkan pada website, layar komputer dan dikirimkan melalui jaringan telekomunikasi.
- (2) Kebijakan manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf d meliputi penetapan prosedur pengendalian keamanan informasi pemerintah daerah.
- (3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 4 huruf b digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah dengan cangkupan aspek meliputi:
 - a. keamanan perangkat teknologi informasi dan 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 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.
- (4) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Bupati.

Pasal 7

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 4 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 SPBE 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.

Pasal 8

- (1) Bupati menetapkan penanggung jawab Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf b dengan Keputusan Bupati.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, Sekretaris Daerah disebut sebagai koordinator SPBE.

Pasal 9

- (1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) menetapkan pelaksana teknis manajemen keamanan informasi SPBE.
- (2) Pelaksana teknis manajemen keamanan informasi 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 dijabat oleh kepala Perangkat Daerah yang membidangi urusan komunikasi dan informatika.
- (4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri atas kepala perangkat daerah atau pejabat administrator yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.
- (5) Tim sebagaimana dimaksud pada ayat 2 ditetapkan dengan Keputusan Bupati.

Pasal 10

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 9 ayat (3) mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah yang meliputi :
 - a. memastikan penerapan standar teknis dan prosedur Keamanan Informasi SPBE;
 - b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi SPBE; dan
 - c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan Informasi SPBE kepada koordinator SPBE.
- (2) Anggota tim sebagaimana dimaksud dalam Pasal 9 ayat (4) 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; dan
- d. berkoordinasi dengan ketua tim terkait perumusan program kerja dan anggaran Keamanan Informasi SPBE

Pasal 11

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c disusun oleh anggota tim keamanan Informasi SPBE dan ditetapkan oleh Ketua Tim.
- (2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan :
 - a. program kerja Keamanan Informasi SPBE yang disusun berdasarkan kategori risiko Keamanan Informasi SPBE; dan
 - b. target realisasi program kerja keamanan Informasi SPBE.

Pasal 12

- (1) Program kerja keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a paling sedikit meliputi :
 - a. edukasi kesadaran keamanan Informasi SPBE;
 - b. penilaian kerentanan Keamanan Aplikasi dan Infrastruktur SPBE;
 - c. peningkatan Keamanan Informasi SPBE;
 - d. penanganan insiden Keamanan Informasi SPBE; dan
 - e. audit Keamanan Informasi SPBE.
- (2) Target realisasi program kerja keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 13

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 huruf d dilakukan oleh koordinator SPBE.
- (2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap :
 - a. sumber daya manusia keamanan informasi SPBE;
 - b. teknologi keamanan informasi SPBE; dan
 - c. anggaran keamanan informasi SPBE.
- (3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya.

Pasal 14

- (1) Sumber daya manusia keamanan informasi sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf a ditempatkan di Perangkat Daerah yang melaksanakan urusan Komunikasi dan Informatika serta memiliki kompetensi :
 - a. keamanan infrastruktur 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 infrastruktur TIK dan keamanan aplikasi; dan/atau
 - b. bimbingan teknis mengenai standar Keamanan Informasi SPBE.
- (3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia keamanan informasi SPBE memiliki kompetensi dan keahlian dalam pelaksanaan Keamanan Informasi SPBE.
- (4) Teknologi keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.
- (5) Anggaran keamanan informasi SPBE sebagaimana dimaksud pada Pasal 13 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundangan-undangan.

Pasal 15

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 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. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan informasi SPBE;
 - b. menetapkan indikator kinerja pada setiap area proses;
 - c. memformulasi pelaksanaan keamanan informasi SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
 - d. menganalisis efektifitas pelaksanaan keamanan informasi SPBE; atau
 - e. mendukung dan merealisasikan program audit keamanan informasi SPBE.
- (4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 16

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 huruf f dilakukan oleh anggota tim Manajemen Keamanan Informasi 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 Manajemen Keamanan Informasi SPBE; dan/atau
 - b. memperbaiki pelaksanaan Manajemen Keamanan Informasi SPBE secara periodik.

Pasal 17

Petunjuk Teknis mengenai Pedoman pelaksanaan Manajemen Keamanan Informasi SPBE ditetapkan dengan Keputusan Bupati

BAB III

MANAJEMEN RISIKO KEAMANAN

Pasal 18

- (1) Untuk mendukung manajemen keamanan informasi di lingkungan Pemerintah Daerah, setiap perangkat daerah dapat menerapkan pengendalian teknis keamanan melalui manajemen risiko.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (risk register) dengan ketentuan substansi meliputi :
 - a. inventarisasi aset elektronik dan non elektronik;
 - b. identifikasi ancaman dan kerentanan keamanan terhadap aset elektronik dan non elektronik;
 - c. penilaian risiko keamanan terhadap aset elektronik dan non elektronik;
 - 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.

BAB IV

PEMBIAYAAN

Pasal 19

Pembiayaan pelaksanaan manajemen Keamanan Informasi SPBE bersumber dari anggaran pendapatan dan belanja daerah.

BAB V
KETENTUAN PENUTUP

Pasal 20

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Tana Paser
pada tanggal 25 November 2025

BUPATI PASER,

ttd

FAHMI FADLI

Diundangkan di Tana Paser
pada tanggal 25 November 2025

SEKRETARIS DAERAH KABUPATEN PASER,

ttd

KATSUL WIJAYA

BERITA DAERAH KABUPATEN PASER TAHUN 2025 NOMOR 35

SALINAN SESUAI DENGAN ASLINYA

KEPALA BAGIAN HUKUM



ANDI AZIS

PEMBINA TK 1

NIP. 19680816 199803 1 007