



KEMENTERIAN HUKUM REPUBLIK INDONESIA
KANTOR WILAYAH JAWA TIMUR
Jalan Kayoon No.50-52, Genteng, Surabaya, Jawa Timur 60271
Telepon:(031)5340707, Faksimile:(031) 5345496
Laman: <http://jatim.kemenkum.go.id>, Pos-el: kanwiljatim@kemenkum.go.id

Nomor : W15-PP.04.02-153
Sifat : Penting
Lampiran : -
Hal : Penyampaian Hasil Pengharmonisasian,
Pembulatan, dan Pemantapan Konsepsi
Rancangan Peraturan Wali Kota Kediri
(Surat Selesai Harmonisasi).

30 Januari 2026

Yth. Wali Kota Kediri
Di Tempat

Menindaklanjuti Surat Pj. Sekretaris Daerah Pemerintah Kota Kediri Nomor: 100.3.2/1692/419.033/2025 Tertanggal 27 November 2025 Perihal Permohonan Pengharmonisasian Pembulatan dan Pemantapan Konsepsi Raperkada, bersama ini kami sampaikan bahwa Rancangan Peraturan Wali Kota Kediri tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Kediri telah dilakukan Pengharmonisasian, Pembulatan, dan Pemantapan Konsepsi sesuai dengan ketentuan Pasal 58 dan Pasal 97D Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan.

Sehubungan hal tersebut maka Rancangan Peraturan Wali Kota dimaksud di atas dapat ditindaklanjuti ke tahapan berikutnya.

Atas perhatian dan kerja samanya diucapkan terima kasih.



Kepala Kantor Wilayah,



Haris Sukamto

Tembusan :

1. Menteri Hukum Republik Indonesia.
2. Direktur Jenderal Peraturan Perundang-undangan Kementerian Hukum.



WALI KOTA KEDIRI
PROVINSI JAWA TIMUR

PERATURAN WALI KOTA KEDIRI
NOMOR TAHUN 2025

TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS
ELEKTRONIK ~~DILINGKUNGAN PEMERINTAH KOTA KEDIRI~~

DENGAN RAHMAT TUHAN YANG MAHA ESA
WALI KOTA KEDIRI,

- Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Daerah, 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 dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
- c. bahwa berdasarkan ketentuan ~~Pasal 2~~ 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, manajemen keamanan informasi SPBE ~~wajib~~ **perlu** dilaksanakan oleh setiap Pemerintah Daerah berdasarkan pedoman yang telah ditetapkan;
- ~~d.~~ bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik ~~Dilingkungan Pemerintah Kota Kediri~~;
- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan dalam Daerah Istimewa Yogyakarta (Berita Negara Republik Indonesia Tahun 1950 Nomor 45) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang Nomor 16 dan Nomor 17 Tahun 1950 tentang Pembentukan Kota-Kota Besar dan Kota-Kota Kecil di Jawa (Lembaran Negara Republik Indonesia Tahun 1954 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 551);

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~~ [UU 9/2015](#) 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 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 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 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 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
12. Peraturan Wali Kota Kediri Nomor 42 Tahun 2019 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kota Kediri Tahun 2020 Nomor 1) sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Wali Kota Kediri Nomor 48 Tahun 2022 tentang Perubahan Kedua Atas Peraturan Walikota Nomor 42 Tahun 2019 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kota Kediri Tahun 2022 Nomor 48);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK ~~DI LINGKUNGAN PEMERINTAH KOTA KEDIRI.~~

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Kediri.
2. Pemerintah Daerah adalah Pemerintah Kota Kediri.
3. Wali Kota adalah Wali Kota Kediri.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Kediri.
5. Perangkat Daerah adalah unsur pembantu Wali Kota dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Dinas Komunikasi dan Informatika Kota Kediri yang selanjutnya disebut Dinas adalah perangkat daerah di lingkungan Pemerintah Kota Kediri yang menyelenggarakan urusan pemerintahan di bidang komunikasi, informatika, statistik, dan persandian.
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, manipulasi, pengelolaan, dan pemindahan informasi antar media.
9. 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.
10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
11. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (~~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 sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

Maksud dan Tujuan Manajemen..

- (1) Peraturan Wali Kota ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di Pemerintah Daerah;.
- (2) Kebijakan internal manajemen keamanan informasi SPBE 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 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.
- (4) Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (~~non-repudiation~~) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE. *Dibuat Tabulasi a,b,c*

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 Daerah yang harus diamankan dalam SPBE.

Pasal 4

- (1) **Penetapan penanggung jawab** sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Wali Kota. *(Wali Kota menetapkan penanggung jawab...)*
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Sekretaris Daerah sebagai penanggung jawab **merupakan ketentuan yang tidak terpisahkan** dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan. *(sesuaikan dengan Pasal 5 Peraturan BSSN No 4/2021)*

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 Dinas.
- (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 Pemerintah Daerah. *(Dijelaskan / disebutkan pimpinan perangkat daerah meliputi siapa saja tambahkan di pasal baru)*
Disarankan tambah ayat (5) untuk penetapan Tim Pelaksana Teknis Keamanan SPBE

Pasal 6

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di Daerah yang meliputi:
 - a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Daerah;
 - b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di Daerah;
 - c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai 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 continuity* dan *disaster recovery plans*; dan *dicari padanan katanya*
 - 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 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 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 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 dalam 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 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 informasi 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 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 Daerah.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
 - a. menganalisis efektivitas 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 III 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 substansi 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 analisis dampak jika terjadi risiko;
 - f. analisa analisis kontrol keamanan yang bisa diterapkan; dan/atau
 - g. rekomendasi kontrol keamanan.
- (3) Prosedur pelaksanaan manajemen risiko mengacu sesuai pada ketentuan peraturan perundang-undangan.

Pasal 14

- (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 informasi SPBE di Daerah dengan cakupan 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. 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.
- (3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan melalui Keputusan Wali Kota 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 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 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 yang 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 paling sedikit 6 (enam) bulan sekali tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV

KETENTUAN PENUTUP

Pasal 17

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Kediri.

Ditetapkan di Kota Kediri
pada tanggal
WALI KOTA KEDIRI,

VINANDA PRAMESWATI

Diundangkan di Kota Kediri
pada tanggal
Pj. SEKRETARIS DAERAH,

MOCHAMAD FERRY DJATMIKO

BERITA DAERAH KOTA KEDIRI TAHUN 2025 NOMOR