WALIKOTA SURABAYA
PROVINSI JAWA TIMUR

SALINAN

PERATURAN WALIKOTA SURABAYA
NOMOR 62 TAHUN 2023

TENTANG

PEDOMAN PELAKSANAAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA SURABAYA

WALIKOTA SURABAYA,

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kota Surabaya, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa berdasarkan ketentuan Pasal 33 Peraturan Walikota Surabaya Nomor 68 Tahun 2020 tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah sebagaimana telah diubah dengan Peraturan Walikota Surabaya Nomor 45 Tahun 2022 tentang Perubahan Atas Peraturan Walikota Surabaya Nomor 68 Tahun 2020 tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah, maka perlu menetapkan Peraturan Walikota tentang Pedoman Pelaksanaan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Walikota tentang Pedoman Pelaksanaan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Surabaya.

Mengingat : 1. Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar Dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan Daerah Istimewa Yogyakarta sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 tentang Perubahan Batas Wilayah Kotapraja Surabaya dan Daerah Tingkat II Surabaya Dengan Mengubah Pembentukan Daerah-daerah Kabupaten Dalam Lingkungan Propinsi Jawa Timur, dan Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar Dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan Daerah Istimewa Yogyakarta (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 2730);

2. 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);

3. 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);

4. Undang-undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

5. 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 diubah beberapa kali terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);

6. 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 9 Tahun 2015 tentang Perubahan Kedua Atas Undang- Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);

7. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);

8. 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);

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

10. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

11. 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);

12. 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);

13. 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);

14. 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);

15. Peraturan Daerah Kota Surabaya Nomor 14 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Surabaya (Lembaran Daerah Kota Surabaya Tahun 2016 Nomor 12, Tambahan Lembaran Daerah Kota Surabaya Nomor 10) sebagaimana telah diubah dengan Peraturan Daerah Kota Surabaya Nomor 3 Tahun 2021 tentang Perubahan Atas Peraturan Daerah Kota Surabaya Nomor 14 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Surabaya (Lembaran Daerah Kota Surabaya Tahun 2021 Nomor 3, Tambahan Lembaran Daerah Kota Surabaya Nomor 3);

16. Peraturan Walikota Surabaya Nomor 68 Tahun 2020 Tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah (Berita Daerah Kota Surabaya Tahun 2020 Nomor 69) sebagaimana telah diubah dengan Peraturan Walikota Surabaya Nomor 45 Tahun 2022 tentang Perubahan Atas Peraturan Walikota Surabaya Nomor 68 Tahun 2020 tentang Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Daerah (Berita Daerah Kota Surabaya Tahun 2022 Nomor 46).

MEMUTUSKAN

Menetapkan : PERATURAN WALIKOTA TENTANG PEDOMAN PELAKSANAAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA SURABAYA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Surabaya.
2. Pemerintah Daerah adalah Pemerintah Daerah Kota Surabaya.
3. Walikota adalah Walikota Surabaya.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Surabaya.

5. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Kepala Daerah 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. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.

10. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (*confidentiality*) atas informasi dan komunikasi secara Elektronik.

11. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.

12. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.

13. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.

14. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau 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.

16. Pihak ketiga adalah semua pihak atau pihak lain selain Pemerintah Daerah, yang memiliki hubungan kontrak dengan Pemerintah Daerah untuk membangun dan mengembangkan aplikasi.

Pasal 2

(1) Peraturan Walikota ini bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak resiko keamanan informasi.

(2) Peraturan Walikota ini dimaksudkan sebagai acuan dalam melaksanakan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kota Surabaya.

(3) Ruang lingkup Peraturan Walikota ini meliputi:

a. penetapan ruang lingkup manajemen keamanan informasi SPBE;

b. penetapan penanggung jawab;

c. perencanaan;

d. dukungan pengoperasian;

e. evaluasi kinerja; dan

f. perbaikan berkelanjutan terhadap keamanan informasi.

(4) Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE dapat menerapkan pengendalian teknis keamanan yang meliputi:

a. manajemen risiko;

b. penetapan prosedur pengendalian keamanan informasi SPBE; dan

c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam pasal 2 ayat (3) 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 (3) huruf b dilaksanakan oleh Walikota.

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.

(3) Dalam melaksanakan tugas sebagai penanggungjawab keamanan SPBE, Sekretaris Daerah disebut 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 sebagai dimaksud pada ayat (1) terdiri atas:

a. pimpinan perangkat daerah yang membidangi urusan komunikasi dan informatika di Pemerintah Daerah, sebagai ketua tim; dan

b. seluruh pimpinan perangkat daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah, sebagai anggota tim.

(3) Ketentuan lebih lanjut mengenai pelaksana teknis Keamanan SPBE sebagai dimaksud pada ayat (2) ditetapkan dengan Keputusan Walikota.

Pasal 6

(1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas:

a. menetapkan prosedur pengendalian keamanan informasi SPBE;

b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Daerah;

c. memastikan penerapan 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 kelangsungan bisnis atau layanan TIK (*business continuity)* dan perencanaan pemulihan bencana terhadap layanan TIK (*disaster 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 peraturan perundang-undangan;

c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen kelangsungan bisnis atau layanan TIK (*business continuity)* dan perencanaan pemulihan bencana terhadap layanan TIK (*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 (3) huruf c ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan oleh pelaksana teknis Keamanan SPBE, 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 pasal 7 ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah dan ketentuan prioritas setiap tahunnya.

Pasal 9

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (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 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 (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. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau

b. mendukung dan merealisasikan program audit Keamanan SPBE.

(4) Dalam rangka pelaksanaan audit keamanan SPBE, Koordinator SPBE dapat melimpahkan kepada pimpinan perangkat daerah yang membidangi urusan pengawasan intern di lingkungan Pemerintah Daerah.

(5) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 12

(1) Perbaikan berkelanjutan terhadap keamanan informasi sebagaimana dimaksud dalam Pasal 2 ayat (3) 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 (4) 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 14

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (4) 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 Kota Surabaya dengan cakupan aspek dapat meliputi:

a. keamanan perangkat teknologi informasi komunikasi;

b. keamanan jaringan;

c. keamanan akses fisik dan logic pusat data;

d. keamanan *remote working;*

e. persayaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;

f. pengelolaan aset;

g. keamanan migrasi data;

h. konfigurasi perangkat IT *Security*;

i. perlindungan data pribadi;

j. keamanan komunikasi;

k. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;

l. pengendalian keamanan informasi terhadap pihak ketiga;

m. penerapan kriptografi;

n. penanganan insiden keamanan informasi;

o. kelangsungan bisnis atau layanan TIK (*business continuity*);

p. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);

q. audit internal keamanan SPBE; dan/atau

r. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk standar operasional prosedur atau surat edaran Sekretaris Daerah selaku Koordinator SPBE.

Pasal 15

(1) Setiap perangkat daerah 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 (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 menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan Pihak ketiga.

(5) Perangkat daerah membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian/kontrak dengan Pihak ketiga.

BAB IV
KETENTUAN PENUTUP

Pasal 17

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Walikota ini dengan penempatannya dalam Berita Pemerintah Kota Surabaya.

Ditetapkan di Surabaya
pada tanggal 20 Juni 2023

WALIKOTA SURABAYA,

ttd

ERI CAHYADI

Diundangkan di Surabaya
pada tanggal 20 Juni 2023

SEKRETARIS DAERAH KOTA SURABAYA,

ttd

Dr. Ikhsan, S.Psi., M.M.
Pembina Utama Madya
NIP 19690809 199501 1 002

BERITA DAERAH KOTA SURABAYA TAHUN 2023 NOMOR 62

Salinan sesuai dengan aslinya,

Ditandatangani secara elektronik oleh :
KEPALA BAGIAN HUKUM DAN KERJASAMA
Sidharta Praditya Revienda Putra, S.H., M.H.
NIP. 197803072005011004