SALINAN

WALIKOTA MOJOKERTO

PROVINSI JAWA TIMUR

PERATURAN WALIKOTA MOJOKERTO

NOMOR 40 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUP PEMERINTAH KOTA MOJOKERTO

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA MOJOKERTO,

Menimbang : a. bahwa dalam rangka melaksanakan ketentuan Pasal 41 Peraturan Walikota Mojokerto Nomor 38 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik, perlu dilaksanakan manajemen keamanan informasi untuk menjamin keberlangsungan Sistem Pemerintahan Berbasis Elektronik di seluruh Perangkat Daerah Lingkup Pemerintah Kota Mojokerto dengan meminimalkan dampak risiko keamanan informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Walikota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkup Pemerintah Kota Mojokerto;

Mengingat : 1. Undang-Undang Nomor 17 Tahun 1950 tentang Pembentukan Daerah Kota Kecil dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang Nomor 16 dan 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);

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 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);
5. 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);
6. Peraturan Pemerintah Nomor 47 Tahun 1982 tentang Perubahan Batas Wilayah Kotamadya Daerah Tingkat II Mojokerto (Lembaran Negara Republik Indonesia Tahun 1982 Nomor 74, Tambahan Lembaran Negara Republik Indonesia Nomor 3242);
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 Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
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 Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
15. Peraturan Daerah Kota Mojokerto Nomor 3 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Kota Mojokerto Tahun 2022 Nomor 3, Tambahan Lembaran Daerah Kota Mojokerto Nomor 2);
16. Peraturan Walikota Mojokerto Nomor 38 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik dalam Penyelenggaraan Pemerintahan Daerah (Berita Daerah Kota Mojokerto Tahun 2021 Nomor 227/D) sebagaimana telah diubah dengan Peraturan Walikota Mojokerto Nomor 35 Tahun 2022 tentang Perubahan Atas Peraturan Walikota Nomor 38 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik Dalam Penyelenggaraan Pemerintahan Daerah (Berita Daerah Kota Mojokerto Tahun 2022 Nomor 35);
17. Peraturan Walikota Mojokerto Nomor 78 Tahun 2022 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika Kota Mojokerto (Berita Daerah Kota Mojokerto Tahun 2022 Nomor 78);

MEMUTUSKAN:

Menetapkan : PERATURAN WALIKOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUP PEMERINTAH KOTA MOJOKERTO.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Kota adalah Kota Mojokerto.
2. Pemerintah Kota adalah Pemerintah Kota Mojokerto.
3. Walikota adalah Walikota Mojokerto.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Mojokerto.
5. Perangkat Daerah adalah unsur pembantu Walikota 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 dengan memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang berkaitan 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 adalah unsur tata kelola SPBE yang 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 kerahasiaan (*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 elekrtonik.

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 *computer* dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
15. Infrastruktur SPBE adalah 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

Peraturan Walikota ini dimaksudkan sebagai kebijakan internal Manajemen Keamanan Informasi SPBE di seluruh Perangkat Daerah di lingkup Pemerintah Kota.

Pasal 3

Tujuan ditetapkannya Peraturan Walikota ini adalah sebagai pedoman pengelolaan Manajemen Keamanan Informasi secara terpadu untuk memastikan terjaganya kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, Infrastruktur SPBE dan Aplikasi SPBE.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 4

(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 dilaksanakan dengan menerapkan pengendalian teknis yang meliputi:
    a. manajemen risiko;

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 4 ayat (1) huruf a meliputi:

a. data dan informasi SPBE;

b. Aplikasi SPBE; dan

c. Infrastruktur SPBE.

(2) Keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:

a. penjaminan Kerahasiaan;

b. penjaminan Keutuhan;

c. penjaminan Ketersediaan;

d. penjaminan keaslian; dan

e. penjaminan kenirsangkalan.

(3) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Kota yang harus diamankan dalam SPBE.

(4) Setiap Perangkat Daerah di lingkungan Pemerintah Kota harus menerapkan Keamanan Informasi SPBE dalam penyelenggaraan SPBE.

Pasal 6

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b dilaksanakan oleh Walikota.

(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 dengan peraturan perundang-undangan.

Pasal 7

(1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 6 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, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkup Pemerintah Kota.

Pasal 8

(1) Ketua tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE di lingkup Pemerintah Kota yang meliputi:

a. menetapkan prosedur pengendalian Keamanan Informasi SPBE Pemerintah Kota;
b. mengevaluasi penerapan prosedur pengendalian Keamanan Infomasi SPBE di lingkungan Pemerintah Kota;
c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan 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 *business continuity* dan *disaster recovery plans*; dan
f. melaporkan pelaksanaan Manajemen Keamanan Informasi SPBE pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 7 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 *business continuity* dan *disaster recovery plans*; dan
d. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 4 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 10

(1) Program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 9 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 11

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 4 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 12

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 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 11 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 13

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf e dilakukan oleh koordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Manajemen Keamanan Informasi SPBE di lingkup Pemerintah Kota.

(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 14

(1) Perbaikan berkelanjutan terhadap keamanan informasi sebagaimana dimaksud dalam Pasal 4 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.

BAB III
PENGENDALIAN TEKNIS KEAMANAN

Pasal 15

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 4 ayat (2) 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 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 16

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 4 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 lingkup Pemerintah Kota dengan cakupan aspek dapat meliputi:
    a. keamanan perangkat TIK;
    b. keamanan jaringan;
    c. keamanan pusat data;
    d. keamanan perangkat *end point*;
    e. keamanan *remote working*;
    f. keamanan penyimpanan elektronik;
    g. pengelolaan *access control*;

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 dalam bentuk Keputusan Walikota, surat edaran Sekretaris Daerah atau kebijakan teknis lainnya.

Pasal 17

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 16 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 18

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf c dilakukan oleh setiap Perangkat Daerah.
(2) Dalam pelaksanaan pengendalian teknis melalui pengelolaan pihak ketiga, Perangkat Daerah harus melakukan kegiatan sebagai berikut:

a. memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
b. memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya;
c. menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Infomasi dalam hubungan kerjasama dengan pihak ketiga; dan
d. membuat layanan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang diisyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV

KETENTUAN PENUTUP

Pasal 19

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Mojokerto
pada tanggal 7 Juli 2023

WALIKOTA MOJOKERTO,

ttd.

IKA PUSPITASARI

Diundangkan di Mojokerto
pada tanggal 7 Juli 2023

SEKRETARIS DAERAH KOTA MOJOKERTO,

ttd.

GAGUK TRI PRASETYO, ATD., M.M.
Pembina Utama Madya
NIP. 19680206 199301 1 002

BERITA DAERAH KOTA MOJOKERTO TAHUN 2023 NOMOR 40

Salinan sesuai dengan aslinya
Kepala Bagian Hukum,

MOKHAMAD TURATMONO, S.H.
Pembina
NIP. 19650704 199302 1 005