



WALI KOTA PEKALONGAN
PROVINSI JAWA TENGAH

PERATURAN WALI KOTA PEKALONGAN
NOMOR 74 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
DI LINGKUNGAN PEMERINTAH KOTA PEKALONGAN

- WALI KOTA PEKALONGAN,
- Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kota Pekalongan, perlu melaksanakan manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik 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 Kota Pekalongan dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik;
- c. bahwa untuk melaksanakan ketentuan pasal 40 Peraturan Daerah Kota Pekalongan Nomor 4 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik, terkait pedoman manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik dan berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis

Elektronik di Lingkungan Pemerintah Kota
Pekalongan;

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 Djawa Timur, Djawa Tengah, Djawa Barat dan Daerah Istimewa Jogjakarta, sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Perubahan Undang-Undang Nomor 16 dan 17 Tahun 1950 tentang Pembentukan Kota-kota besar dan Kota-Kota Ketjil di Djawa (Lembaran Negara Republik Indonesia Tahun 1954 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 551);
3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintah 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 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. Peraturan Pemerintah Nomor 21 Tahun 1988 tentang Perubahan Batas Wilayah Kabupaten Daerah Tingkat II Pekalongan dan Kabupaten Daerah Tingkat II Batang (Lembaran Negara Republik Indonesia Tahun 1988 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 3381);
5. Peraturan Daerah Kota Pekalongan Nomor 4 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Kota Pekalongan Tahun 2021 Nomor 4);

MEMUTUSKAN:

Menetapkan

: PERATURAN WALI KOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA PEKALONGAN

BAB I KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Pekalongan.
2. Wali Kota adalah Wali Kota Pekalongan.
3. Pemerintah Daerah adalah Wali Kota sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Pekalongan.
5. Perangkat Daerah adalah unsur pembantu Wali Kota dan DPRD 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 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 Elektronik.
13. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
14. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara, dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.

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.
17. Indeks KAMI adalah aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001.

Pasal 2

Peraturan Wali Kota ini dimaksudkan sebagai pedoman penyelenggaraan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kota Pekalongan untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

Pasal 3

Ruang lingkup Peraturan Wali Kota ini meliputi:

- a. kebijakan internal Manajemen Keamanan Informasi SPBE;
- b. pengendalian teknis keamanan; dan
- c. kategori Sistem Elektronik dan proses penilaian mandiri.

Pasal 4

- (1) Penyelenggaraan Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 dilaksanakan dengan menerapkan Sistem Manajemen Keamanan Informasi sesuai SNI ISO/IEC 27001:2022.
- (2) Pedoman penyelenggaraan 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 penyelenggaraan Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi :
 - a. manajemen risiko;
 - b. penetapan kebijakan dan prosedur pengendalian Keamanan Informasi SPBE; dan
 - c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN
KEAMANAN INFORMASI SPBE

Bagian Kesatu
Penetapan Ruang Lingkup

Pasal 5

- (1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 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 Kota Pekalongan yang harus diamankan dalam SPBE.

Bagian Kedua
Penetapan Penanggung Jawab

Pasal 6

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b dilaksanakan oleh Wali Kota.
- (2) Penanggungjawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah Kota Pekalongan.
- (3) Sekretaris Daerah Kota Pekalongan 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 dijabat oleh kepala Perangkat Daerah yang menyelenggarakan urusan pemerintah

daerah di bidang Komunikasi dan Informatika atau kepala Perangkat Daerah yang menyelenggarakan urusan Pemerintah Daerah di bidang persandian.

- (4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh kepala Perangkat Daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Kota Pekalongan.

Pasal 8

- (1) Ketua tim sebagaimana dimaksud dalam pasal 7 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kota Pekalongan yang meliputi:
 - a. menyusun kebijakan dan prosedur pengendalian Keamanan Informasi SPBE Pemerintah Kota Pekalongan;
 - b. mengevaluasi penerapan kebijakan dan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Pemerintah Kota Pekalongan;
 - 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 kebijakan dan 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.

Bagian Ketiga
Perencanaan

Pasal 9

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf c dilakukan 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 Pasal 9 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Bagian Keempat
Dukungan Pengoperasian

Pasal 11

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 4 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 12

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada Pasal 11 ayat (2) huruf a paling sedikit harus 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 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 pada Pasal 11 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.
- (5) Anggaran Keamanan SPBE sebagaimana dimaksud pada pasal 11 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima Evaluasi Kinerja

Pasal 13

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf e dilakukan oleh koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kota Pekalongan.
- (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.

Bagian Keenam Perbaikan Berkelanjutan

Pasal 14

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 4 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 15

- (1) Manajemen risiko sebagaimana dimaksud dalam Pasal 4 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 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) Kebijakan dan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada Pasal 4 ayat (3) huruf b disusun oleh ketua tim pelaksana teknis Keamanan SPBE.
- (2) Penetapan kebijakan dan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kota Pekalongan dengan cakupan aspek dapat meliputi:
 - a. keamanan perangkat TIK;
 - b. keamanan jaringan dan komunikasi;
 - 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. manajemen aset;
 - k. manajemen SDM;
 - l. manajemen perubahan;
 - m. keamanan migrasi data;
 - n. konfigurasi perangkat *IT Security*;
 - o. perlindungan data pribadi;
 - p. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
 - q. pengendalian Keamanan Informasi terhadap pihak ketiga;
 - r. penerapan kriptografi;
 - s. penanganan insiden Keamanan Informasi;
 - t. kelangsungan bisnis atau layanan TIK (*business continuity*);
 - u. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
 - v. audit internal keamanan SPBE; dan/atau
 - w. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.
- (3) Kebijakan dan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk Keputusan Wali Kota atau surat edaran Sekretaris Daerah atau kebijakan teknis lainnya.

Pasal 17

- (1) Setiap Perangkat Daerah harus melaksanakan kebijakan dan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada 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 (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 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 rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi 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.

BAB IV KATEGORI SISTEM ELEKTRONIK DAN PROSES PENILAIAN MANDIRI

Pasal 19

- (1) Kategori sistem elektronik berdasarkan asas Risiko terdiri atas:
 - a. sistem elektronik strategis;
 - b. sistem elektronik tinggi; dan
 - c. sistem elektronik rendah.
- (2) Sistem elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.
- (3) Sistem elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b merupakan sistem elektronik yang berdampak terbatas pada kepentingan sektor dan atau Daerah tertentu.
- (4) Sistem elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c merupakan sistem elektronik lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

Pasal 20

- (1) Kategorisasi sistem elektronik sebagaimana dimaksud dalam Pasal 19 dilakukan secara mandiri oleh Perangkat Daerah yang memiliki sistem elektronik.
- (2) Format penilaian mandiri sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 21

- (1) Untuk mempersiapkan penerapan SMKI sebagaimana dimaksud dalam Pasal 2 ayat (2), Perangkat Daerah dapat melakukan penilaian mandiri berdasarkan kategorisasi sistem elektronik menggunakan Indeks KAMI;
- (2) Ketentuan mengenai Indeks KAMI dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
PENUTUP

Pasal 22

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 Pekalongan.

Ditetapkan di Pekalongan
pada tanggal 2 Oktober 2023

WALI KOTA PEKALONGAN,


ACHMAD AZZAN ARSLAN DJUNAID