



WALI KOTA PEKALONGAN
PROVINSI JAWA TENGAH

PERATURAN WALI KOTA PEKALONGAN
NOMOR 58 TAHUN 2021

TENTANG
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI
LINGKUNGAN PEMERINTAH KOTA PEKALONGAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA PEKALONGAN,

- Menimbang : a. bahwa dalam rangka melindungi informasi di pemerintah Kota Pekalongan, perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;
- b. bahwa untuk melaksanakan ketentuan Pasal 35 ayat (2) Peraturan Daerah Kota Pekalongan Nomor 4 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik dan berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a perlu menetapkan Peraturan Wali Kota tentang Penyelenggaraan Persandian untuk Pengamanan Informasi 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 Djogjakarta 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 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 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587), sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Tahun 2020 Nomor 245, Tambahan Lembaran Negara Nomor 6573);
5. Peraturan Daerah Kota Pekalongan Nomor 4 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Daerah Kota Pekalongan Tahun 2021 Nomor 4).

- Memperhatikan :
1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
 2. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah;

MEMUTUSKAN :

Menetapkan : PERATURAN WALI KOTA TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI 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. Perangkat Daerah adalah unsur pembantu Wali Kota dan DPRD dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
5. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan daerah di bidang persandian.
6. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah profesi bagi pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang bekerja pada instansi pemerintah.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah suatu sistem tata kelola pemerintahan yang memanfaatkan teknologi informasi secara menyeluruh dan terpadu dalam pelaksanaan

- administrasi pemerintahan dan penyelenggaraan pelayanan publik pada Pemerintah Daerah.
8. Persandian adalah kegiatan di bidang pengamanan data atau informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kriptografi beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terikat pada etika profesi sandi.
 9. Informasi adalah keterangan, pernyataan, gagasan dan tanda-tanda yang mengandung nilai, makna dan pesan baik data, fakta maupun penjelasannya yang dapat dilihat, didengar dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun non-elektronik.
 10. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
 11. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
 12. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan digital dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
 13. Sistem Elektronik adalah serangkaian perangkat dan prosedur yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi yang dikelola di lingkungan Pemerintah Daerah.
 14. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
 15. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.

BAB II MAKSUD DAN TUJUAN

Bagian Kesatu Maksud

Pasal 2

Peraturan Wali Kota ini dimaksudkan sebagai pedoman bagi Pemerintah Daerah dalam menyelenggarakan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah.

Bagian Kedua Tujuan

Pasal 3

Peraturan Wali Kota ini bertujuan untuk :

- a. menciptakan harmonisasi dalam melaksanakan urusan pemerintahan daerah di bidang Persandian;
- b. memberikan pedoman bagi Pemerintah Daerah dalam menyelenggarakan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah;
- c. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar Perangkat Daerah di lingkungan Pemerintah Daerah.

BAB III RUANG LINGKUP

Pasal 4

Ruang lingkup Peraturan Wali Kota ini meliputi:

- a. penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah; dan
- b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

BAB IV PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

Bagian Kesatu Umum

Pasal 5

Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 4 huruf a dilaksanakan melalui:

- a. penyusunan kebijakan Pengamanan Informasi;
- b. pengelolaan sumber daya Keamanan Informasi;
- c. pengamanan Sistem Elektronik dan pengamanan informasi non-elektronik; dan
- d. penyediaan layanan Keamanan Informasi.

Bagian Kedua Penyusunan Kebijakan Pengamanan Informasi

Pasal 6

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf a dilakukan dengan:

- a. menyusun rencana strategis pengamanan informasi;
- b. menetapkan arsitektur Keamanan Informasi; dan
- c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 7

- (1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf a ditetapkan oleh Wali Kota.

- (2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
- (3) Rencana strategis Pengamanan Informasi berlaku untuk jangka waktu 5 (lima) tahun.
- (4) Rencana strategis Pengamanan Informasi terdiri atas:
 - a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun; dan
 - b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun.
- (5) Rencana strategis Pengamanan Informasi yang telah disusun diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
- (6) Dalam melakukan penyusunan rencana strategis Pengamanan Informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Pasal 8

- (1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf b ditetapkan oleh Wali Kota.
- (2) Penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
- (3) Arsitektur Keamanan Informasi paling sedikit memuat:
 - a. infrastruktur teknologi informasi;
 - b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
 - c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
- (4) Arsitektur Keamanan Informasi berlaku untuk jangka waktu (lima) tahun.
- (5) Arsitektur Keamanan Informasi dilakukan evaluasi oleh Wali Kota pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.
- (6) Dalam melakukan penyusunan Arsitektur Keamanan Informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada lembaga Pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Pasal 9

- (1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf c ditetapkan oleh Wali Kota.
- (2) Penyusunan tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
- (3) Aturan mengenai tata kelola Keamanan Informasi terdiri atas:
 - a. keamanan sumber daya teknologi informasi;
 - b. keamanan akses kontrol;
 - c. keamanan data dan informasi;
 - d. keamanan sumber daya manusia;
 - e. keamanan jaringan;
 - f. keamanan surat elektronik;

- g. keamanan pusat data; dan/atau
 - h. keamanan komunikasi
- (4) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada lembaga Pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Bagian Ketiga Pengelolaan Sumber daya Keamanan Informasi

Pasal 10

- (1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf b dilaksanakan oleh Dinas.
- (2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
- a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
 - b. pengelolaan sumber daya manusia; dan
 - c. manajemen pengetahuan.

Pasal 11

- (1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
- (2) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 12

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b dilakukan oleh Dinas.
- (2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
- a. pengembangan kompetensi;
 - b. pembinaan karir;
 - c. pendayagunaan; dan
 - d. pemberian tunjangan pengamanan persandian.

Pasal 13

- (1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf a dilaksanakan dengan :
- a. melalui tugas belajar, pendidikan dan pelatihan, pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, workshop, seminar dan kegiatan lainnya yang terkait

- pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;
- b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian, pihak lainnya, atau Pemerintah Daerah; dan
 - c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.
- (2) Pembinaan karir sebagaimana dimaksud dalam pasal 12 ayat (2) huruf b dilaksanakan dengan :
- a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
 - b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.
- (3) Pendayagunaan sebagaimana dimaksud dalam pasal 12 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan;
- (4) Pemberian tunjangan pengamanan persandian sebagaimana dimaksud dalam pasal 12 ayat (2) huruf d adalah pemberian tunjangan khusus kepada Aparatur Sipil Negara yang diangkat sebagai pengelola pengamanan persandian di lingkungan Pemerintah Daerah yang lingkup tugas dan tanggung jawabnya meliputi bidang pengamanan persandian sesuai dengan ketentuan Peraturan Perundang-undangan;
- (5) Pemberian tunjangan pengamanan persandian ditetapkan dengan keputusan Wali Kota atas usulan kepala Dinas.

Pasal 14

- (1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilakukan oleh Dinas.
- (2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait keamanan Informasi.
- (3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi.
- (4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi.
- (5) Dalam pelaksanaan manajemen pengetahuan, Dinas dapat melakukan koordinasi dan konsultasi dengan lembaga Pemerintah yang menyelenggarakan urusan pemerintahan di bidang keamanan siber dan persandian

Bagian Keempat

Pengelolaan Sistem Elektronik dan Pengamanan Informasi Non-elektronik

Pasal 15

Pengamanan sistem elektronik dan pengamanan informasi non-elektronik sebagaimana dimaksud dalam pasal 5 huruf (c) dilaksanakan oleh Dinas sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 16

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam pasal 15 terdiri atas:

- a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan terhadap data dan informasi;
- b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data Pemerintah Daerah, jaringan intra Pemerintah Daerah, dan sistem penghubung layanan Pemerintah Daerah; dan
- c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 17

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16, Dinas melakukan:
 - a. identifikasi;
 - b. deteksi;
 - c. proteksi; dan
 - d. penanggulangan dan pemulihan.
- (2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.
- (3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.
- (4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan melalui kegiatan mitigasi risiko dan penerapan perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.
- (5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan melalui kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 18

- (1) Dalam mendukung pelaksanaan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 17, Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi;
- (2) Pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) disesuaikan dengan standar yang ditetapkan oleh BSSN.
- (3) Pusat operasi Pengamanan Informasi bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 19

- (1) Pengamanan informasi non-elektronik sebagaimana dimaksud dalam Pasal 15 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi non-elektronik.
- (2) Pengamanan Informasi non-elektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Pasal 20

- (1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
- (2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
- (3) Audit Keamanan Informasi dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 21

- (1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf d dilaksanakan oleh Dinas.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
 - a. Wali Kota dan Wakil Wali Kota;
 - b. Perangkat Daerah;
 - c. Aparatur Sipil Negara pada Pemerintah Daerah; dan
 - d. Pihak lainnya.

Pasal 22

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam pasal 21 ayat (1) meliputi:

- a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
- b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
- c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
- d. perlindungan Informasi melalui penyediaan perangkat teknologi Keamanan Informasi dan jaring komunikasi sandi;
- e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
- f. audit Keamanan Sistem Elektronik;
- g. audit keamanan pelaksanaan sistem manajemen;
- h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan pemerintah daerah dan publik;
- i. peningkatan kompetensi sumber daya manusia di bidang Keamanan Informasi dan/atau persandian;
- j. pengelolaan pusat operasi Pengamanan Informasi;

- k. penanganan insiden Keamanan Sistem Elektronik;
- l. perlindungan Informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
- m. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
- n. jenis Layanan Keamanan Informasi lainnya.

Pasal 23

- (1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 22, Dinas melaksanakan manajemen Layanan Keamanan Informasi.
- (2) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.
- (3) Manajemen Layanan Keamanan Informasi merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan.
- (4) Manajemen Layanan Keamanan Informasi dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi.

BAB V

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 24

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 4 huruf b ditetapkan oleh Wali Kota.
- (2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) bertujuan untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.
- (3) Jaring komunikasi sandi internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
 - a. Jaring komunikasi sandi antar Perangkat Daerah;
 - b. Jaring komunikasi sandi internal Perangkat Daerah; dan
 - c. Jaring komunikasi sandi Pimpinan Daerah.
- (4) Jaring komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
- (5) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.
- (6) Jaring komunikasi sandi Pimpinan Daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Wali Kota, Wakil Wali Kota, dan Kepala Perangkat Daerah.

Pasal 25

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 24 ayat (1) dilaksanakan melalui:
 - a. identifikasi pola hubungan komunikasi sandi; dan
 - b. analisis pola hubungan komunikasi sandi.

- (2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
 - a. pola hubungan komunikasi pimpinan dan pejabat struktural Pemerintah Daerah;
 - b. alur informasi yang dikomunikasikan antar Perangkat Daerah dan internal Perangkat Daerah;
 - c. teknologi informasi dan komunikasi;
 - d. infrastruktur komunikasi; dan
 - e. kompetensi personel.
- (3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).
- (4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
 - a. pengguna Layanan yang akan terhubung dalam jaring komunikasi sandi;
 - b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan;
 - c. perangkat keamanan teknologi informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
- (5) Hasil analisis pola hubungan komunikasi sandi ditetapkan sebagai Pola Hubungan Komunikasi Sandi Antar Perangkat Daerah dalam bentuk Keputusan Wali Kota.
- (6) Keputusan Wali Kota sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
 - a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;
 - b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
 - c. sarana dan prasarana yang digunakan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
- (7) Salinan Keputusan Wali Kota disampaikan oleh Wali Kota kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala Lembaga Pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

BAB VI PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 26

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.
- (2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas setiap 1(satu) tahun sekali.
- (3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi kepada Wali Kota dan kepada Gubernur sebagai wakil Pemerintah Pusat.

Pasal 27

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII PEMBIAYAAN

Pasal 28

Pembiayaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah bersumber dari Anggaran Pendapatan dan Belanja Daerah serta sumber pembiayaan lainnya yang sah sesuai ketentuan peraturan perundang-undangan.

BAB VIII PENUTUP

Pasal 29

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 07 Oktober 2021

WALI KOTA PEKALONGAN


ACHMAD AFZAN ARSLAN DJUNAID