WALIKOTA SERANG
PROVINSI BANTEN

PERATURAN WALIKOTA SERANG
NOMOR 31 TAHUN 2018

TENTANG

PENYELENGGARAAN PERSANDIAN DALAM PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH KOTA SERANG

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA SERANG,

Menimbang :

a. bahwa pemerintah daerah wajib mengelola informasi publik yang dimilikinya;
b. bahwa untuk melindungi informasi publik perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan b, perlu menetapkan Peraturan Walikota tentang Penyelenggaraan Persandian Dalam Pengamanan Informasi di Lingkungan Pemerintah Kota Serang;

Mengingat :

1. Undang-Undang Nomor 32 Tahun 2007 tentang Pembentukan Kota Serang di Provinsi Banten (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 98, Tambahan Lembaran Negara Republik Indonesia Nomor 4748);
2. 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);
3. 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);
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 beberapa kali diubah, 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. Peraturan .....

5. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
6. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887);
7. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara sebagaimana telah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara;
8. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaring Komunikasi Peralatan Sandi;
9. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah (Berita Negara Republik Indonesia Tahun 2012 Nomor 808);
10. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi dan Kabupaten /Kota(Berita Negara Republik Indonesia Tahun 2017 Nomor 758);
11. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik (Berita Negara Republik Indonesia Tahun 2017 Nomor 907);
12. Peraturan Daerah Kota Serang Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Serang (Lembaran Daerah Kota Serang Tahun 2016 Nomor 7;

MEMUTUSKAN :

Menetapkan : PERATURAN WALIKOTA TENTANG PENYELENGGARAAN PERSANDIAN DALAM PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KOTA SERANG

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini, yang dimaksud dengan :

1. Daerah adalah Kota Serang.
2. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan oleh pemerintah daerah dan dewan perwakilan rakyat daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

3. Pemerintah .....

3. Pemerintah Daerah adalah Walikota sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom;
4. Walikota adalah Walikota Serang;
5. Perangkat Daerah adalah unsur pembantu Walikota dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah;
6. Dinas adalah Dinas Komunikasi dan Informatika yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan informatika, bidang statistik dan bidang persandian.
7. Urusan Pemerintahan adalah kekuasaaan pemerintahan yang menjadi kewenangan Presiden yang pelaksanaannya dilakukan oleh kementerian negara dan penyelenggara Pemerintah Daerah untuk melindungi, melayani, memberdayakan, dan menyejahterakan masyarakat.
8. Pejabat Pengelola Informasi dan Dokumentasi adalah pejabat yang bertanggung jawab di bidang penyimpanan, pendokumentasian, penyediaan, dan/atau pelayanan informasi di badan publik.
9. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
10. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
11. 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 ataupun nonelektronik.
12. Informasi Publik adalah Informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang serta Informasi lain yang berkaitan dengan kepentingan publik.
13. Informasi Berklasifikasi adalah Informasi Publik yang dikecualikan menurut ketentuan peraturan perundang-undangan.
14. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subyek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Balai Sertifikasi Elektronik Lembaga Sandi Negara.
15. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memilki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

16. Otoritas .....

16. Otoritas Pendaftaran adalah petugas yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon pemilik Sertifikat Elektronik.
17. *Virtual Private Netwo*rk yang selanjutnya disingkat *VPN* adalah suatu koneksi antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan internet.
18. *Jamming* adalah kegiatan untuk mengacak sinyal di waktu dan tempat tertentu.
19. *Security Operation Center* yang selanjutnya disebut *SOC* adalah kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.
20. *Network Operation Center* yang selanjutnya disebut *NOC* Adalah tempat administrator yang mengawasi, memantau dan mengamankan jaringan komunikasi. Berupa sebuah ruangan yang berisi visualisasi dari jaringan atau jaringan yang sedang dipantau, *workstation* di mana status rinci jaringan dapat dilihat, dan perangkat lunak yang diperlukan untuk mengelola jaringan.

Pasal 2

Penyelenggaraan Persandian merupakan penjabaran atas pelaksanaan kebijakan, program, dan kegiatan bidang Persandian.

BAB II
TANGGUNG JAWAB PEMERINTAH DAERAH

Pasal 3

(1) Walikota memimpin dan bertanggung jawab atas penyelenggaraan Persandian yang menjadi kewenangan Daerah.
(2) Walikota menetapkan kebijakan dalam penyelenggaraan persandian untuk pengamanan informasi sesuai dengan kewenangannya.
(3) Walikota mendelegasikan kewenangan kepada Dinas bertanggung jawab atas kinerja pelaksanaan urusan pemerintahan bidang persandian sesuai dengan tugas dan fungsinya.

Pasal 4

(1) Dinas menyusun perencanaan penyelenggaraan Persandian sesuai dengan kewenangannya.
(2) Perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam perencanaan pembangunan daerah.
(3) Perencanaan pembangunan daerah sebagaimana dimaksud pada ayat (2) merupakan bagian integral dari sistem perencanaan pembangunan nasional dan dituangkan dalam dokumen perencanaan pembangunan daerah.

(4) Dokumen .....

(4) Dokumen perencanaan pembangunan daerah sebagaimana dimaksud pada ayat (3) berupa rencana pembangunan jangka panjang daerah, rencana pembangunan jangka menengah daerah, dan rencana kerja pemerintah daerah.

Pasal 5

(1) Dalam menjabarkan rencana pembangunan jangka menengah daerah sebagaimana dimaksud dalam Pasal 4 ayat (4), Dinas menyusun rencana strategis Dinas yang memuat tujuan, sasaran, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan informasi di Daerah.

(2) Dalam menjabarkan rencana kerja pemerintah daerah sebagaimana dimaksud dalam Pasal 4 ayat (4), Dinas menyusun rencana kerja Dinas yang memuat program, kegiatan, lokasi, dan kelompok sasaran berdasarkan layanan urusan pemerintahan bidang Persandian, disertai indikator kinerja program dan kegiatan, serta penganggaran penyelenggaraan Persandian untuk pengamanan informasi di Daerah.

BAB III
PENGELOLAAN DAN PERLINDUNGAN INFORMASI

Bagian Kesatu

Umum

Pasal 6

Pengelolaan informasi publik untuk proses pengiriman dan penerimaan dokumen dapat melalui jaringan yang aman atau VPN.

Pasal 7

Perlindungan informasi publik dapat menggunakan sertifikat elektronik yang dikeluarkan oleh Badan Siber dan Sandi Negara.

Bagian Kedua
Pengelolaan Informasi Publik Yang Dikecualikan

Pasal 8

Penentuan informasi publik maupun yang dikecualikan dikeluarkan oleh PPID Kota Serang dalam bentuk keputusan Walikota yang mengacu pada Peraturan perundang-undangan.

Pasal 9

Pengelolaan Informasi Publik yang dikecualikan di Daerah meliputi:
a. pembuatan;
b. pemberian label;
c. pengiriman; dan
d. penyimpanan.

Paragraf 1
Pembuatan Informasi Publik yang dikecualikan

Pasal 10

Pembuatan Informasi Publik yang dikecualikan sebagaimana dimaksud dalam Pasal 9 huruf a dilakukan dengan ketentuan:

a. Informasi Publik yang Dikecualikan dibuat oleh pemilik atau pengelola informasi dengan menggunakan sarana dan prasarana yang aman;
b. perangkat yang digunakan untuk membuat dan/atau mengkomunikasikan Informasi Publik yang Dikecualikan harus milik dinas dan hanya dimanfaatkan untuk kepentingan dinas;
c. konsep Informasi Publik yang Dikecualikan tidak boleh disimpan dan harus dihancurkan secara fisik maupun lojik;
d. dokumen Elektronik yang berisi Informasi Publik yang Dikecualikan yang sudah disahkan disimpan dalam bentuk yang tidak dapat diubah atau dimodifikasi; dan
e. penggandaan dan/atau pengubahan Informasi Publik yang Dikecualikan harus dengan ijin dari pemilik atau pengelola informasi.

Paragraf 2
Pemberian label Informasi Publik Yang Dikecualikan

Pasal 11

(1) Pemberian label dikecualikan sebagaimana dimaksud dalam Pasal 9 huruf b harus sesuai dengan tingkat kerahasiaan informasinya, serta bergantung pada bentuk dan media penyimpanannya.
(2) Tingkat kerahasiaan informasi sebagaimana dimaksud pada ayat (1) di suatu Perangkat Daerah harus diperlakukan sama tingkat kerahasiaannya oleh Perangkat Daerah lainnya.

Pasal 12

Label sebagaimana dimaksud dalam Pasal 11 diberikan dengan ketentuan:

a. dokumen cetak:
    1. ditulis dengan cap berwarna merah pada bagian atas dan bawah setiap halaman; dan
    2. dalam hal dokumen cetak sebagaimana dimaksud pada huruf a disalin, cap label pada salinan harus menggunakan warna yang sama dengan warna cap pada dokumen asli;
b. ditulis pada baris *subject* pada *header* surat elektronik;
c. diberikan dalam metadata Dokumen Elektronik, sistem atau aplikasi; dan/atau
d. media penyimpanan:
    1. ditempelkan pada fisik media penyimpanan;
    2. terlihat dengan jelas;
    3. media penyimpanan yang telah diberi label dibungkus sekali lagi tanpa diberi label; dan
    4. label harus muncul saat informasi yang tersimpan di dalamnya diakses.

Paragraf 3 .....

Paragraf 3
Pengiriman Informasi Publik yang Dikecualikan

Pasal 13

Pengiriman Informasi Publik yang dikecualikan sebagaimana dimaksud dalam Pasal 9 huruf c dilakukan dengan ketentuan:

a. pengiriman dan penerimaan Informasi Publik yang dikecualikan di Daerah harus menggunakan persandian;
b. pengiriman dan penerimaan Informasi Publik yang dikecualikan di Daerah dilaksanakan di kamar sandi oleh petugas sandi; dan
c. pengiriman dokumen cetak yang berisi Informasi Publik yang dikecualikan dilakukan dengan memasukkannya ke dalam dua amplop, yaitu:
    1. amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (kilat, sangat segera, segera, dan biasa); dan
    2. amplop pertama sebagaimana dimaksud pada angka 1 dimasukkan ke dalam amplop kedua dengan tanda yang sama kecuali cap klasifikasi.

Pasal 14

Informasi Publik yang dikecualikan disimpan dalam bentuk Dokumen Elektronik dan/atau dokumen cetak.

Paragraf 4
Penyimpanan Informasi Publik yang Dikecualikan

Pasal 15

Penyimpanan Informasi Publik yang dikecualikan dalam bentuk Dokumen Elektronik sebagaimana dimaksud dalam Pasal 14 dilakukan dengan ketentuan:

a. diamankan dengan persandian;
b. lokasi penyimpanan harus dilengkapi kendali akses untuk mencegah risiko kehilangan, kerusakan, dan manipulasi data;
c. tidak boleh disimpan di dalam komputer, *mobile devices*, atau media penyimpanan pribadi;
d. membuat data cadangan (*back up*) secara berkala; dan
e. media penyimpanan dilarang digunakan, dipinjam, atau dibawa keluar ruangan atau keluar kantor tanpa ijin pengelola informasi.

Pasal 16

Penyimpanan Informasi Publik yang dikecualikan dalam bentuk dokumen cetak sebagaimana dimaksud dalam Pasal 14 dilakukan dengan ketentuan:

a. lokasi penyimpanan harus dilengkapi kendali akses untuk mencegah risiko kehilangan dan kerusakan;
b. disimpan dalam brankas yang memiliki kunci kombinasi atau media penyimpanan yang aman; dan
c. diarsip secara khusus dengan tertib dan rapi sesuai prosedur arsip yang berlaku.

Bagian Ketiga .....

Bagian Ketiga
Perlindungan Informasi Publik Yang Dikecualikan

Pasal 17

Perlindungan Informasi Publik yang dikecualikan di lingkungan Pemerintah Kota Serang meliputi:

a. perlindungan fisik;
b. perlindungan administrasi; dan
c. perlindungan lojik.

Pasal 18

Perlindungan fisik sebagaimana dimaksud dalam Pasal 17 huruf a dilakukan melalui:

a. kendali akses ruang;
b. pemasangan teralis;
c. penggunaan kunci ganda;
d. pemasangan kamera pengawas; dan/atau
e. penggunaan ruang tempest.

Pasal 19

(1) Perlindungan administrasi sebagaimana dimaksud dalam Pasal 17 huruf b dilakukan untuk mencegah kelalaian dan tindakan indisipliner.
(2) Perlindungan administrasi sebagaimana dimaksud pada ayat (1) dilakukan melalui penguatan standar dan operasional prosedur dalam pengamanan Informasi Publik yang Dikecualikan.

Pasal 20

Perlindungan lojik sebagaimana dimaksud dalam Pasal 17 huruf c dilakukan dengan menggunakan persandian untuk menjamin aspek kerahasiaan, keutuhan, otentikasi, dan nir penyangkalan.

BAB IV
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 21

Penyelenggaraan JKS untuk pengamanan Informasi Publik yang dikecualikan diterapkan melalui penetapan pola hubungan komunikasi sandi.

Pasal 22

Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 21 dilakukan melalui tahapan:

a. identifikasi;
b. analisis;
c. koordinasi;
d. penetapan.

Pasal 23

Identifikasi yang dilakukan untuk menentukan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 22 huruf a meliputi:

a. identifikasi .....

a. identifikasi terhadap pola hubungan komunikasi pejabat/pimpinan di Daerah yang sedang dilaksanakan;
b. identifikasi terhadap alur informasi yang dikomunikasikan antar Perangkat Daerah;
c. identifikasi terhadap sarana dan prasarana teknologi informasi dan komunikasi yang digunakan oleh pejabat/pimpinan di Pemerintah daerah;
d. identifikasi terhadap infrastruktur komunikasi yang ada di Daerah dan di lingkungan kantor Perangkat Daerah; dan
e. identifikasi terhadap kompetensi personil yang dibutuhkan.

Pasal 24

(1) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 22 huruf b dilakukan berdasarkan hasil identifikasi pola hubungan komunikasi sandi.
(2) Analisis sebagaimana dimaksud pada ayat (1) dapat dilengkapi dengan data kebutuhan anggaran dalam periode waktu satu tahun anggaran.

Pasal 25

Dinas mengkoordinasikan hasil identifikasi dan analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 23 dan Pasal 24 ke Badan Siber dan Sandi Negara untuk melihat dan menjamin keterhubungan secara vertikal.

Pasal 26

(1) Pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 21 ditetapkan dengan Keputusan Walikota.
(2) Pola hubungan komunikasi sandi yang akan ditetapkan sebagaimana dimaksud pada ayat (1) paling sedikit berisi:
    a. entitas yang terhubung; dan
    b. tugas dan tanggung jawab setiap entitas terhadap fasilitas dan layanan yang diberikan.

Pasal 27

Setiap pejabat yang telah ditetapkan sebagai entitas dalam pola hubungan komunikasi sandi harus menggunakan peralatan sandi dalam melakukan setiap komunikasi yang mengandung Informasi Publik yang Dikecualikan.

BAB V
PENGELOLAAN SUMBER DAYA PERSANDIAN

Pasal 28

Pengelolaan sumber daya persandian terdiri dari:
a. pengelolaan sumber daya manusia; dan
b. pengelolaan sarana dan prasarana.

Pasal 29

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 28 huruf a meliputi perencanaan dan pengembangan sumber daya manusia.

(2) Dalam .....

(2) Dalam hal pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1), Daerah memberikan kompensasi atas tanggung jawab dalam melaksanakan tugas di bidang persandian untuk pengamanan informasi.

(3) Kompensasi sebagaimana dimaksud pada ayat (2) berupa:

a. pemberian tunjangan; dan

b. pengusulan pemberian tanda penghargaan bidang Persandian.

(4) Tunjangan sebagaimana dimaksud pada ayat (3) meliputi Tunjangan Pengamanan Persandian dan tunjangan jabatan fungsional sandiman.

(5) Kompensasi sebagaimana dimaksud pada ayat (3) diberikan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 30

Perencanaan sumber daya manusia sebagaimana dimaksud dalam Pasal 29 ayat (1) disusun dengan ketentuan:

a. memperhatikan jumlah dan kompetensi sumber daya manusia yang dibutuhkan sesuai dengan hasil analisis beban kerja serta formasi jabatan; dan

b. mengusulkan kebutuhan sumber daya manusia kepada Badan Kepegawaian Daerah.

Pasal 31

Pengembangan sumber daya manusia sebagaimana dimaksud dalam Pasal 29 ayat (1) dilakukan melalui:

a. pendidikan dan pelatihan fungsional sandiman;

b. pendidikan dan pelatihan teknis sandi; dan/atau

c. bimbingan teknis atau seminar atau asistensi atau lokakarya terkait dengan Persandian dan teknologi informasi serta bidang ilmu lain yang dibutuhkan.

Pasal 32

(1) Pengelolaan sarana dan prasarana sebagaimana dimaksud dalam Pasal 28 huruf b meliputi:

a. materiil sandi;

b. JKS;

c. alat pendukung utama Persandian; dan

d. tempat kegiatan sandi.

(2) Ketentuan mengenai pengelolaan sarana dan prasarana mengacu kepada Peraturan Kepala Lembaga Sandi Negara.

BAB VI
PENYELENGGARAAN OPERASIONAL DUKUNGAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

Pasal 33

Kegiatan operasional dukungan persandian untuk pengamanan informasi di Daerah dilaksanakan oleh Pegawai Negeri Sipil yang memiliki kualifikasi sandi.

Pasal 34 .....

Pasal 34

Kegiatan operasional dukungan persandian untuk pengamanan informasi sebagaimana dimaksud dalam Pasal 33 meliputi:

a. *jamming*;
b. kontra penginderaan;
c. penilaian keamanan sistem informasi; dan/atau
d. penyelenggaraan *SOC*.

Pasal 35

(1) Kegiatan *jamming* sebagaimana dimaksud dalam Pasal 34 huruf a dilakukan untuk mencegah terungkapnya Informasi Publik yang Dikecualikan kepada pihak yang tidak berhak selama berlangsungnya rapat terbatas Perangkat Dearah.
(2) Kegiatan *jamming* dapat dilakukan berdasarkan hasil identifikasi kegiatan-kegiatan yang berpotensi untuk timbulnya ancaman dan gangguan terhadap penyalahgunaan sinyal.
(3) Pelaksanaan kegiatan *jamming* untuk pengamanan informasi di Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 36

(1) Kegiatan kontra penginderaan sebagaimana dimaksud dalam Pasal 34 huruf b bertujuan untuk mencegah adanya pengawasan dari pihak yang tidak berhak terhadap Informasi Publik yang Dikecualikan yang disampaikan oleh Perangkat Dearah.
(2) Kegiatan kontra penginderaan sebagaimana dimaksud pada ayat (1) dilakukan terhadap ruangan-ruangan yang digunakan oleh Perangkat Dearah untuk penyampaian Informasi Publik yang Dikecualikan.
(3) Ruangan sebagaimana dimaksud pada ayat (2) dapat berupa ruang kerja, ruang rapat, dan/atau rumah dinas/jabatan.

Pasal 37

Temuan hasil kegiatan kontra penginderaan berupa barang yang diduga menjadi peralatan penginderaan (*surveillance*) dapat dikonsultasikan ke Badan Siber dan Sandi Negara.

Pasal 38

Kegiatan kontra penginderaan sebagaimana dimaksud dalam Pasal 36 dilakukan secara berkala.

Pasal 39

Pelaksanaan kegiatan kontra penginderaan untuk pengamanan informasi di Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 40

(1) Kegiatan penilaian keamanan sistem informasi sebagaimana dimaksud dalam Pasal 34 huruf c dilakukan untuk mengukur tingkat kerawanan dan keamanan informasi di Daerah.
(2) Kegiatan penilaian keamanan sistem informasi dilaksanakan dengan melakukan pemeriksaan terhadap ada atau tidaknya celah kerawananan pada sistem informasi di Daerah.

Pasal 41 .....

Pasal 41

(1) Daerah melakukan kegiatan penilaian keamanan sistem informasi secara mandiri.
(2) Dalam hal Daerah tidak dapat melakukan kegiatan penilaian keamanan sistem informasi secara mandiri sebagaimana dimaksud pada ayat (1), Daerah mengajukan permohonan penilaian keamanan sistem informasi kepada Badan Siber dan Sandi Negara.
(3) Pelaksanaan kegiatan penilaian Keamanan Sistem Informasi di Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 42

(1) *SOC* sebagaimana dimaksud dalam Pasal 34 huruf d adalah kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.
(2) Penyelenggaraan *SOC* bertujuan untuk mencegah dan menanggulangi ancaman keamanan informasi dengan berkolaborasi bersama *network operation center* Pemerintah Daerah yang telah terbangun infrastrukturnya.

Pasal 43

Infrastruktur *SOC* Daerah dapat terpusat dan terhubung dengan Badan Siber dan Sandi Negara.

Pasal 44

(1) Penyelenggaraan *SOC* di Daerah dilakukan secara mandiri dengan tetap berkerjasama dengan Badan Siber dan Sandi Negara.
(2) Penyelenggaraan *SOC* di Daerah sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII
PENGGUNAAN SERTIFIKAT ELEKTRONIK

Pasal 45

Penggunaan Sertifikat Elektronik di Daerah dilaksanakan atas dasar kebutuhan pengamanan terhadap informasi dan sistem elektronik serta pelaksanaan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 46

(1) Penggunaan Sertifikat Elektronik di Daerah dilaksanakan untuk mendukung sistem pemerintahan berbasis elektronik (*e-government*).
(2) Penggunaan Sertifikat Elektronik di Daerah bertujuan :
    a. meningkatkan kapabilitas dan tata kelola keamanan informasi dalam penyelenggaraan sistem elektronik;
    b. meningkatkan keamanan informasi dan sistem elektronik;
    c. meningkatkan kepercayaan dan penerimaan terhadap implementasi sistem elektronik;
    d. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.

BAB VIII .....

BAB VIII
PENGAWASAN DAN EVALUASI

Pasal 47

Pengawasan dan evaluasi penyelenggaraan Persandian dimaksudkan untuk memantau perkembangan, mengidentifikasi hambatan, dan upaya perbaikan dalam penyelenggaraan Persandian untuk pengamanan informasi di Daerah.

Pasal 48

Pengawasan dan evaluasi penyelenggaraan Persandian di Daerah sebagaimana dimaksud dalam Pasal 47 dilaksanakan oleh Dinas guna meningkatkan kinerja Persandian.

Pasal 49

Pengawasan dan evaluasi penyelenggaraan Persandian sebagaimana dimaksud dalam Pasal 48 meliputi:

a. pengawasan dan evaluasi yang bersifat rutin dan insidentil; dan
b. pengawasan dan evaluasi yang bersifat tahunan.

Pasal 50

Pengawasan dan evaluasi yang bersifat rutin dan insidentil sebagaimana dimaksud dalam Pasal 49 huruf a terdiri dari:

a. pemantauan penggunaan materiil sandi, aplikasi sandi, dan/atau fasilitas layanan Persandian lainnya di Daerah; dan
b. pelaksanaan kebijakan manajemen risiko penyelenggaraan Persandian di Daerah.

Pasal 51

Pengawasan dan evaluasi yang bersifat tahunan sebagaimana dimaksud dalam Pasal 49 huruf b terdiri dari:

a. pengukuran tingkat pemanfaatan layanan Persandian oleh Perangkat Daerah;
b. penilaian mandiri terhadap penyelenggaraan Persandian pada Pemerintah Daerah;
c. pengukuran tingkat kepuasan Perangkat Daerah terhadap layanan Persandian yang dikelola oleh Dinas Komunikasi dan Informatika ; dan
d. penyusunan Laporan Penyelenggaraan Persandian Tahunan Pemerintah Kota Serang.

BAB IX
PELAPORAN

Pasal 52

(1) Laporan hasil evaluasi penyelenggaraan Persandian untuk pengamanan informasi Pemerintah Daerah disampaikan oleh Walikota kepada Presiden melalui Menteri Dalam Negeri dan tembusan kepada Kepala Badan Siber dan Sandi Negara.

(2) Laporan hasil evaluasi sebagaimana dimaksud pada ayat (1) memuat capaian kinerja urusan pemerintahan bidang Persandian.

(3) Dalam .....

(3) Dalam hal tertentu yang dianggap penting terkait teknis Persandian, Walikota dapat menyampaikan laporan langsung kepada Kepala Badan Siber dan Sandi Negara.

BAB X
PEMBIAYAAN

Pasal 53

Pembiayaan penyelenggaraan Persandian untuk pengamanan informasi di Daerah bersumber dari Anggaran Pendapatan dan Belanja Daerah Kota Serang.

BAB XI
KETENTUAN LAIN-LAIN

Pasal 54

Dalam rangka pelaksanaan urusan pemerintahan bidang persandian, Dinas Komunikasi dan Informatika dapat melaksanakan koordinasi dan/atau konsultasi ke Badan Siber dan Sandi Negara, Perangkat Daerah terkait maupun antar Pemerintah Daerah lainnya.

BAB XII
KETENTUAN PENUTUP

Pasal 55

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Serang
pada tanggal 10 Oktober 2018

PENJABAT WALIKOTA SERANG,

Ttd

ADE ARIYANTO

Diundangkan di Serang
pada tanggal 11 Oktober 2018

SEKRETARIS DAERAH KOTA SERANG,

Ttd

Tb. URIP HENUS

BERITA DAERAH KOTA SERANG TAHUN 2018 NOMOR 31

Salinan Sesuai Dengan Aslinya
KEPALA BAGIAN HUKUM,

Ttd

YUDI SURYADI
NIP. 19671010 1988011 1 002