



BUPATI MAJALENGKA
PROVINSI JAWA BARAT

PERATURAN BUPATI MAJALENGKA

NOMOR 66 TAHUN 2021

TENTANG

TATA KELOLA KEAMANAN INFORMASI DAN JARING KOMUNIKASI SANDI
DI LINGKUNGAN PEMERINTAH DAERAH KABUPATEN MAJALENGKA

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MAJALENGKA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 8 ayat (1) dan Pasal 24 Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah, perlu menetapkan Peraturan Bupati tentang Tata Kelola Keamanan Informasi dan Jaring Komunikasi Sandi di Lingkungan Pemerintah Daerah Kabupaten Majalengka.

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Propinsi Djawa Barat (Berita Negara Republik Indonesia Tahun 1950) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1968 tentang Pembentukan Kabupaten Purwakarta dan Kabupaten Subang dengan Mengubah Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Propinsi Djawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);

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 2

4. 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);
5. 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);
6. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
7. 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);
8. Peraturan Presiden Nomor 27 Tahun 2014 Tentang Jaringan Informasi Spasial (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 78);
9. Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
10. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
11. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaring Komunikasi Peralatan Sandi;
12. 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);
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 Kepala Lembaga Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik (Berita Negara Republik Indonesia Tahun 2017 Nomor 907);
15. Peraturan Daerah 3

15. Peraturan Daerah Kabupaten Majalengka Nomor 14 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Majalengka (Lembaran Daerah Kabupaten Majalengka Tahun 2016 Nomor 14) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Majalengka Nomor 12 Tahun 2019 tentang Perubahan Atas Peraturan Daerah Kabupaten Majalengka Nomor 14 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Majalengka (Lembaran Daerah Kabupaten Majalengka Tahun 2019 Nomor 12);
16. Peraturan Bupati Majalengka Nomor 42 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas Pokok dan Fungsi Dinas Daerah di Lingkungan Pemerintah Kabupaten Majalengka (Berita Daerah Kabupaten Majalengka Tahun 2019 Nomor 42) sebagaimana telah diubah dengan Peraturan Bupati Majalengka Nomor 110 Tahun 2020 tentang Perubahan Atas Peraturan Bupati Majalengka Nomor 42 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas Pokok dan Fungsi Dinas Daerah di Lingkungan Pemerintah Kabupaten Majalengka (Berita Daerah Kabupaten Majalengka Tahun 2020 Nomor 113);
17. Peraturan Bupati Majalengka Nomor 28 Tahun 2020 tentang Rincian Tugas, Fungsi dan Tata Kerja Komunikasi dan Informatika Kabupaten Majalengka (Berita Daerah Kabupaten Majalengka Tahun 2020 Nomor 28)
18. Peraturan Bupati Majalengka Nomor 13 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Majalengka (Berita Daerah Kabupaten Majalengka Tahun 2021 Nomor 13).

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG TATA KELOLA KEAMANAN INFORMASI DAN JARING KOMUNIKASI SANDI DI LINGKUNGAN PEMERINTAH DAERAH KABUPATEN MAJALENGKA.

**BAB I
KETENTUAN UMUM**

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan :

1. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
2. Daerah Kabupaten adalah yang selanjutnya disebut Daerah adalah Daerah Kabupaten Majalengka.

3. Pemerintahan 4

3. Pemerintahan Daerah adalah penyelenggara 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.
4. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
5. Bupati adalah Bupati Majalengka.
6. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam menyelenggarakan urusan pemerintahan yang menjadi kewenangan daerah.
7. Dinas adalah Dinas yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan informatika, bidang statistik dan bidang persandian.
8. Urusan Pemerintahan adalah kekuasaan pemerintahan yang menjadi kewenangan Presiden yang pelaksanaannya dilakukan oleh kementerian negara dan penyelenggara Pemerintah Daerah untuk melindungi, melayani, memberdayakan, dan menyejahterakan masyarakat.
9. Pejabat Pengelola Informasi dan Dokumentasi adalah pejabat yang bertanggung jawab di bidang penyimpanan, pendokumentasian, penyediaan, dan/atau pelayanan informasi di badan publik.
10. 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.
11. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi;
12. 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 non elektronik.
13. 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.
14. Informasi Berklasifikasi adalah Informasi Publik yang dikecualikan menurut ketentuan peraturan perundang-undangan.
15. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tandatangan elektronik dan identitas yang menunjukkan status subyek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara Sertifikat Elektronik.

16. 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 memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
17. 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.
18. *Virtual Private Network* yang selanjutnya disingkat VPN adalah suatu koneksi antara satu jaringan dengan jaringan lain secara pribadi melalui jaringan internet.
19. Jamming adalah kegiatan untuk mengacak sinyal di waktu dan tempat tertentu.
20. *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.
21. *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) Bupati memimpin dan bertanggung jawab atas penyelenggaraan Persandian yang menjadi kewenangan Daerah.
- (2) Bupati menetapkan kebijakan dalam penyelenggaraan persandian untuk pengamanan informasi sesuai dengan kewenangannya.
- (3) Bupati mendelegasikan kewenangan kepada Dinas untuk 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 6

- (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 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 Penyelenggara Sertifikat Elektronik.

Bagian Kedua Pengelolaan Informasi Publik Yang Dikecualikan

Pasal 8

Penentuan informasi publik maupun yang dikecualikan dilakukan oleh Bupati melalui Keputusan Bupati tetapi tidak boleh bertentangan dengan Pedoman Pengelolaan Informasi dan Dokumentasi (PPID) Daerah.

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 logik;
- 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 perubahan Informasi Publik yang Dikecualikan harus dengan izin dari pemilik atau pengelola informasi.

Paragraf 2

Pemberian label Informasi Publik Yang Dikecualikan

Pasal 11

- (1) Pemberian label dikecualikan sebagaimana dimaksud dalam Pasal 10 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

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

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

Perlindungan Informasi Publik Yang Dikecualikan

Pasal 17

Perlindungan Informasi Publik yang dikecualikan di lingkungan Pemerintah Daerah 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; dan
- d. penetapan.

Pasal 23

Identifikasi yang dilakukan untuk menentukan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 21 huruf a meliputi:

- 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 21 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 mengoordinasikan 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 Bupati.
- (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 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 pengelola sandi.
- (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 Perangkat Daerah yang membidangi urusan kepegawaian dan pengembangan sumber daya manusia.

Pasal 31

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

- a. pendidikan dan pelatihan fungsional pengelola sandi;
- 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 12

- 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

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 Daerah.
- (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 Daerah.
- (2) Kegiatan kontra penginderaan sebagaimana dimaksud pada ayat (1) dilakukan terhadap ruangan-ruangan yang digunakan oleh Perangkat Daerah 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 kerawanan pada sistem informasi di Daerah.

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 NOC 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
PENGUNAAN 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
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 insidental; dan
- b. pengawasan dan evaluasi yang bersifat tahunan.

Pasal 50

Pengawasan dan evaluasi yang bersifat rutin dan insidental 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; dan
- d. penyusunan Laporan Penyelenggaraan Persandian Tahunan Pemerintah Daerah.

BAB IX PELAPORAN

Pasal 52

- (1) Laporan hasil evaluasi penyelenggaraan Persandian untuk pengamanan informasi Pemerintah Daerah disampaikan oleh Bupati 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 hal tertentu yang dianggap penting terkait teknis Persandian, Bupati 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.

BAB XI
KETENTUAN LAIN-LAIN

Pasal 54

Dalam rangka pelaksanaan urusan pemerintahan bidang persandian, Dinas 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 Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahui, memerintahkan pengundangan Peraturan Bupati ini dengan menempatkannya dalam Berita Daerah Kabupaten Majalengka.

Ditetapkan di Majalengka
pada tanggal 10 Desember 2021

BUPATI MAJALENGKA,

ttd

KARNA SOBAHI

Diundangkan di Majalengka
pada tanggal 10 Desember 2021

SEKRETARIS DAERAH
KABUPATEN MAJALENGKA,

ttd

EMAN SUHERMAN

BERITA DAERAH KABUPATEN MAJALENGKA TAHUN 2021 NOMOR 66

Salinan sesuai dengan aslinya,

KABALA BAGIAN HUKUM
SEKRETARIAT DAERAH
KABUPATEN MAJALENGKA,

DEWI SUPENA NURBAHAR
NIP. 19651225 198603 1 003

