



BUPATI KUANTAN SINGINGI
PROVINSI RIAU
PERATURAN BUPATI KUANTAN SINGINGI
NOMOR 50 TAHUN 2022

TENTANG
TATA KELOLA KEAMANAN INFORMASI DAN JARING KOMUNIKASI SANDI
DILINGKUNGAN PEMERINTAH DAERAH KABUPATEN KUANTAN SINGINGI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KUANTAN SINGINGI,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 8 ayat (1) dan Pasal 24 ayat (1) 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 Kuantan Singingi;

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

2. Undang-Undang Nomor 53 Tahun 1999 tentang Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir, Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Kuantan Singingi, dan Kota Batam (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 181, Tambahan Lembaran Negara Republik Indonesia Nomor 3902) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 34 Tahun 2008 tentang Perubahan Ketiga atas Undang-Undang Nomor 53 Tahun 1999 tentang

Pembentukan Kabupaten Pelalawan, Kabupaten Rokan Hulu, Kabupaten Rokan Hilir, Kabupaten Siak, Kabupaten Karimun, Kabupaten Natuna, Kabupaten Kuantan Singingi, dan Kota Batam (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 107, Tambahan Lembaran Negara Republik Indonesia Nomor 4880);

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 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 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah dengan Undang – Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Tahun 2022 Nomor 143, Tambahan Lembaran Negara Nomor 6801);
6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5589) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Pemerintahan

Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5670);

7. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
8. 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);
9. Peraturan Presiden Nomor 27 Tahun 2014 tentang Jaringan Informasi Spasial (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 78);
10. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
11. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
12. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaring Komunikasi Peralatan Sandi;
13. 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);
14. 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);
15. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik

(Berita Negara Republik Indonesia Tahun 2017 Nomor 907);

16. Peraturan Bupati Kuantan Singingi Nomor 13 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kuantan Singingi;

MEMUTUSKAN

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

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan :

1. Daerah adalah Daerah Kabupaten Kuantan Singingi.
2. Bupati adalah Bupati Kuantan Singingi.
3. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Pemerintahan Daerah adalah penyelenggara urusan pemerintahan oleh pemerintah 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.
5. Perangkat Daerah adalah unsur pembantu Bupati dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Dinas adalah Dinas yang menyelenggarakan urusan pemerintahan bidang Statistik dan Persandian,
7. 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.

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 kriptografi 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 non elektronik.
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 tandatangan elektronik dan identitas yang menunjukkan status subyek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara Sertifikat Elektronik.
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 computer atau sistem elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, symbol atau ferforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
16. Otoritas Pendaftaran adalah petugas yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaharuan atau pencabutan Sertifikat

Elektronik yang diajukan oleh pemilik atau calon pemilik Sertifikat Elektronik.

17. *Virtual Private Network* 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 dimana status rinci jaringan dapat dilihat dan perangkat lunak yang diperlukan untuk mengelola jaringan.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

Peraturan Bupati ini di susun dengan maksud untuk memberikan pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan penyelenggaraan Persandian untuk pengamanan informasi.

Pasal 3

Penyelenggaraan-Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah bertujuan :

- a. menciptakan harmonisasi dalam penyelenggaraan persandian;
- b. sebagai acuan dalam melaksanakan tata cara penyelenggaraan persandian untuk pengamanan informasi; dan
- c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi.

BAB III

TANGGUNG JAWAB PEMERINTAH DAERAH

Pasal 4

- (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 tugas dan fungsinya.

Pasal 5

- (1) Dinas menyusun perencanaan penyelenggaraan Persandian sesuai dengan kewenangannya.
- (2) Perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) diintegrasikan kedalam 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 Jangka Menengah Daerah sebagaimana dimaksud pada ayat (3) berupa Rencana Pembangunan Jangka Panjang Daerah, Rencana Pembangunan Jangka Menengah Daerah dan Rencana Kerja Perangkat Daerah.

Pasal 6

- (1) Dalam menjabarkan Rencana Pembangunan Jangka Menengah Daerah sebagaimana dimaksud dalam Pasal 5 ayat (4), Dinas menyusun rencana strategis Dinas yang memuat tujuan, sasaran, program dan kegiatan penyelenggaraan Persandian untuk pengamanan informasi Daerah.
- (2) Dalam menjabarkan Rencana Kerja Pemerintah Daerah sebagaimana dimaksud dalam Pasal 5 ayat (4), Dinas penyusunan rencana kerja Dinas yang memuat program, kegiatan, lokasi dan kelompok sasaran berdasarkan layanan urusan-urusan pemerintah bidang persandian, disertai indikator kinerja program dan kegiatan, serta penganggaran penyelenggaraan Persandian untuk pengamanan informasi di Daerah.

BAB IV
PENGELOLAAN DAN PERLINDUNGAN INFORMASI

Bagian Kesatu
Umum

Pasal 7

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

Pasal 8

Perlindungan informasi publik dapat menggunakan sertifikat elektronik yang dikeluarkan oleh Penyelenggara Sertifikat Elektronik.

Bagian Kedua
Pengelolaan Informasi Publik Yang Dikecualikan

Pasal 9

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

Pasal 10

Pengelolaan Informasi Publik yang dikecualikan di Daerah meliputi :

- a. pembuatan;
- b. pemberian label;
- c. pengiriman; dan
- d. penyimpanan.

Bagian Ketiga
Pembuatan Informasi Publik Yang Dikecualikan

Pasal 11

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 izin dari pemilik atau pengelola informasi.

Bagian Keempat

Pemberian Label Informasi Publik Yang Dikecualikan

Pasal 12

- (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 kerahasiaanya oleh Perangkat Daerah lainnya.

Pasal 13

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 subjek 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 saat informasi yang tersimpan didalamnya diakses.

Pasal 14

Pengiriman Informasi Publik yang dikecualikan sebagaimana dimaksud dalam Pasal 10 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 di Daerah dilakukan dengan memasukkannya ke dalam dua amplop, yaitu :
 1. amplop 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 maksud pada angka 1 dimasukan kedalam amplop kedua dengan tanda yang sama kecuali cap klasifikasi.

Pasal 15

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

Bagian Kelima

Penyimpanan Informasi Publik yang Dikecualikan

Pasal 16

Penyimpanan Informasi Publik yang dikecualikan disimpan dalam bentuk Dokumen Elektronik sebagaimana dimaksud dalam Pasal 15 dilakukan dengan ketentuan :

- a. diamankan dengan persandian;
- b. lokasi penyimpanan harus dilengkapi kendali akses untuk mencegah resiko kehilangan, kerusakan dan manipulasi data;
- c. tidak boleh disimpan didalam 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 izin pengelola informasi.

Pasal 17

Penyimpanan Informasi Publik yang dikecualikan dalam bentuk dokumen cetak sebagaimana dimaksud dalam Pasal 15 dilakukan dengan ketentuan :

- a. lokasi penyimpanan harus dilengkapi kendali akses untuk mencegah resiko 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 Keenam

Perlindungan Informasi Publik Yang Dikecualikan

Pasal 18

Perlindungan Informasi Publik yang dikecualikan dilingkungan Pemerintah Daerah meliputi :

- a. perlindungan fisik;
- b. perlindungan administrasi; dan
- c. perlindungan logik.

Pasal 19

Perlindungan fisik sebagaimana dimaksud dalam Pasal 18 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 20

- (1) Perlindungan administrasi sebagaimana dimaksud dalam Pasal 18 huruf b dilakukan untuk mencegah kelalaian dan tindakan indisipliner.
- (2) Perlindungan administrasi sebagaimana dimaksud pada ayat (1) dilakukan melalui penguatan standard dan operasional prosedur dalam pengamanan Informasi Publik yang dikecualikan.

Pasal 21

Perlindungan lojik sebagaimana dimaksud dalam Pasal 18 huruf c dilakukan dengan menggunakan persediaan untuk menjamin aspek kerahasiaan, keutuhan, otentikasi dan nir penyangkalan.

BAB V

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 22

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

Pasal 23

Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 22 dilakukan melalui tahapan :

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

Pasal 24

Identifikasi yang dilakukan untuk menentukan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 23 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 dilingkungan kantor Perangkat Daerah; dan
- e. identifikasi terhadap kompetensi personil yang dibutuhkan.

Pasal 25

- (1) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 23 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 26

Dinas mengkoordinasikan hasil identifikasi dan analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 24 dan Pasal 25 ke Badan Siber dan Sandi Negara untuk melihat dan menjamin keterhubungan secara vertikal.

Pasal 27

- (1) Pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 23 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 28

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 VI

PENGELOLAAN SUMBER DAYA PERSANDIAN

Pasal 29

Pengelolaan Sumber Daya Persandian terdiri dari:

- a. pengelolaan sumber daya manusia; dan
- b. pengelolaan sarana dan prasarana.

Pasal 30

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 29 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 Statistik dan Persandian untuk pengamanan informasi.

- (3) Kompensasi sebagaimana dimaksud pada ayat (2) berupa :
 - a. pemberian tunjangan; dan
 - b. pengusulan pemberian tanda penghargaan pada Statistik dan 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 31

Perencanaan sumber daya manusia sebagaimana dimaksud dalam Pasal 30 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 32

Pengembangan sumber daya manusia sebagaimana dimaksud dalam Pasal 30 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 33

(1) Pengelolaan sarana dan prasarana sebagaimana dimaksud dalam Pasal 29 huruf b meliputi :

- a. materiil sandi;
- b. Jaringan Komunikasi Sandi (JKS);
- c. alat pendukung utama Persandian; dan

d. tempat kegiatan sandi.

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

BAB VII

PENYELENGGARAAN OPERASIONAL DUKUNGAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Pasal 34

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

Pasal 35

Kegiatan operasional dukungan persandian untuk pengamanan informasi sebagaimana dimaksud dalam Pasal 34 meliputi :

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

Pasal 36

- (1) Kegiatan *jamming* sebagaimana dimaksud dalam Pasal 35 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 penyalagunaan sinyal.
- (3) Pelaksanaan kegiatan jamming untuk pengamanan informasi di Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 37

- (1) Kegiatan kontra penginderaan sebagaimana dimaksud dalam Pasal 35 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 38

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

Pasal 39

Kegiatan kontra penginderaan sebagaimana dimaksud dalam Pasal 35 huruf b dilakukan secara berkala.

Pasal 40

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

Pasal 41

- (1) Kegiatan penilaian keamanan sistem informasi sebagaimana dimaksud dalam Pasal 35 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 42

- (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 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 43

- (1) *Security Operation Center* (SOC) sebagaimana dimaksud dalam Pasal 35 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* (NOC) Pemerintah Daerah yang telah membangun infrastrukturnya.

Pasal 44

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

Pasal 45

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

BAB VIII

PENGGUNAAN SERTIFIKAT ELEKTRONIK

Pasal 46

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

Pasal 47

- (1) Pengamanan Sertifikat Elektronik di Daerah dilaksanakan untuk mendukung Sistem Pemerintahan Berbasis Elektronik (*e-government*).
- (2) Penggunaan Sertifikat Elektronik di Daerah bertujuan :
 - a. meningkatkan kapasitas 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; dan
- d. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.

BAB IX

PENGAWASAN DAN EVALUASI

Pasal 48

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

Pasal 49

Pengawasan dan evaluasi penyelenggaraan Persandian di Daerah sebagaimana dimaksud dalam Pasal 48 dilaksanakan oleh Dinas guna meningkatkan kinerja Persandian.

Pasal 50

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 51

Pengawasan dan evaluasi yang bersifat rutin dan insidental sebagaimana dimaksud dalam Pasal 50 huruf a terdiri dari :

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

Pasal 52

Pengawasan dan evaluasi yang bersifat tahunan sebagaimana dimaksud dalam Pasal 50 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 X

PELAPORAN

Pasal 53

- (1) Laporan hasil evaluasi penyelenggaraan Persandian dan 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 Statistik dan Persandian.
- (3) Dalam hal tertentu yang dianggap penting terkait teknis Persandian, Bupati dapat menyampaikan laporan langsung kepada Kepala Badan Siber dan Sandi Negara.

BAB XI

PEMBIAYAAN

Pasal 54

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

BAB XII

KETENTUAN LAIN – LAIN

Pasal 55

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

BAB XIII
KETENTUAN PENUTUP

Pasal 56

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Teluk Kuantan
pada tanggal 16 November 2022

Plt. BUPATI KUANTAN SINGINGI,

ttd.

H. SUHARDIMAN AMBY

Diundangkan di Teluk Kuantan
pada tanggal 16 November 2022

SEKRETARIS DAERAH
KABUPATEN KUANTAN SINGINGI,

ttd.

H. DEDY SAMBUDI

BERITA DAERAH KABUPATEN KUANTAN SINGINGI TAHUN 2022 NOMOR 50

Salinan sesuai dengan aslinya
Plt. KEPALA BAGIAN HUKUM,



IRWAN NAZIF, SH., MH
Pembina Tk. I
NIP. 19680226 199503 1 003