



GUBERNUR KALIMANTAN TENGAH
PERATURAN GUBERNUR KALIMANTAN TENGAH
NOMOR 11 TAHUN 2018
TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH PROVINSI KALIMANTAN TENGAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR KALIMANTAN TENGAH,

- Menimbang : a. bahwa berdasarkan Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah beberapa kali diubah dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah Provinsi merupakan Urusan Pemerintahan Wajib yang tidak berkaitan dengan pelayanan dasar yang menjadi kewenangan Pemerintah Daerah Provinsi;
- b. bahwa setiap pemerintah daerah wajib mengelola informasi yang dimilikinya dan untuk melindungi informasi perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Gubernur tentang Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Kalimantan Tengah;
- Mengingat : 1. Undang-Undang Nomor 21 Tahun 1958 tentang Penetapan Undang-Undang Darurat Nomor 10 Tahun 1957 Tentang Pembentukan Daerah Swatantra Tingkat I Kalimantan Tengah dan Perubahan Undang-undang Nomor 25 Tahun 1956 tentang Pembentukan Daerah-Daerah Swatantra Tingkat I Kalimantan Barat, Kalimantan Selatan dan Kalimantan Timur (Lembaran Negara Republik Indonesia Tahun 1957 Nomor 53, Tambahan Lembaran Negara Republik Indonesia Nomor 1284) Sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 62, Tambahan Lembaran Negara Republik Indonesia Nomor 1622);

2. 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);
3. 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);
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 beberapa kali 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 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 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
7. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100);
8. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaringan Komunikasi Sandi (Berita Negara Republik Indonesia Tahun 2010 Nomor 292);
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 Pemerintahan 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 Komisi Informasi Nomor 1 Tahun 2017 tentang Pengklasifikasian Informasi Publik (Berita Negara Republik Indonesia Tahun 2017 Nomor 429);
13. Peraturan Daerah Provinsi Kalimantan Tengah Nomor 4 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Kalimantan Tengah (Lembaran Daerah Provinsi Kalimantan Tengah Tahun 2016 Nomor 4) sebagaimana telah diubah dengan Peraturan Daerah Provinsi Kalimantan Tengah Nomor 1 Tahun 2018 tentang Perubahan Atas Peraturan Daerah Provinsi Kalimantan Tengah Nomor 4 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Kalimantan Tengah (Lembaran Daerah Provinsi Kalimantan Tengah Tahun 2018 Nomor 1, Tambahan Lembaran Daerah Provinsi Kalimantan Tengah Nomor 90);
14. Peraturan Gubernur Kalimantan Tengah Nomor 43 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Kalimantan Tengah (Berita Daerah Provinsi Kalimantan Tengah Tahun 2016 Nomor 43);

MEMUTUSKAN:

Menetapkan : **PERATURAN GUBERNUR TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI KALIMANTAN TENGAH.**

BAB I KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Provinsi adalah Provinsi Kalimantan Tengah.
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 Daerah adalah Kepala Daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan Urusan Pemerintahan yang menjadi kewenangan daerah otonom.

4. Pemerintah Provinsi adalah Pemerintah Provinsi Kalimantan Tengah.
5. Gubernur adalah Gubernur Kalimantan Tengah.
6. Perangkat Daerah yang selanjutnya disebut PD adalah unsur pembantu Gubernur dalam penyelenggaraan Pemerintahan Daerah yang terdiri atas sekretariat daerah, sekretariat dewan perwakilan rakyat daerah, dinas daerah dan badan daerah dalam lingkup pemerintah Provinsi.
7. 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.
8. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
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 ataupun nonelektronik.
10. 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.
11. Informasi Berklasifikasi adalah Informasi yang telah ditetapkan dan apabila diketahui oleh pihak yang tidak berhak dapat membahayakan keamanan nasional.
12. Tingkat Kerahasiaan Informasi adalah tingkatan yang ditentukan dan ditetapkan terhadap Informasi Berklasifikasi berdasarkan akibat yang dapat ditimbulkan bila Informasi tersebut diketahui oleh pihak yang tidak berhak mengetahuinya.
13. Kawat Instruksi yang selanjutnya disebut KINS adalah informasi atau berita dari instansi yang membuat kunci sistem sandi yang berisi mengenai penetapan pemberlakuan penggunaan kunci sistem sandi tertentu.

14. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
15. 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 pada Badan Siber dan Sandi Negara.
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. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan Informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.
18. Otoritas Sertifikat Digital Badan Siber dan Sandi Negara yang selanjutnya disebut OSD Badan Siber dan Sandi Negara adalah sistem elektronik yang berfungsi sebagai layanan sertifikasi elektronik di Lembaga Sandi Negara.
19. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara OSD Badan Siber dan Sandi Negara yang berada di bawah dan bertanggung jawab kepada Kepala Lembaga Sandi Negara.

Pasal 2

Peraturan Gubernur ini dimaksudkan sebagai acuan bagi Pemerintah Provinsi Kalimantan Tengah dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi di Pemerintah Provinsi Kalimantan Tengah.

Pasal 3

Peraturan Gubernur ini bertujuan:

- a. menciptakan harmonisasi dalam bidang Persandian di Pemerintah Provinsi Kalimantan Tengah;

- b. membantu Kabupaten/Kota dalam melaksanakan tata cara penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Kabupaten/Kota;
- c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi; dan
- d. meningkatkan kinerja Dinas yang menangani Urusan Pemerintahan Bidang Persandian untuk pengamanan informasi.

Pasal 4

Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintahan Provinsi Kalimantan Tengah meliputi:

- a. pengelolaan dan perlindungan informasi berklasifikasi dan informasi publik;
- b. pengelolaan sumber daya persandian;
- c. penyediaan kebutuhan penyelenggaraan persandian untuk pengamanan informasi melalui identifikasi dan analisis pola hubungan komunikasi sandi;
- d. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi;
- e. pemanfaatan layanan sertifikat elektronik;
- f. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh PD; dan
- g. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

Pasal 5

Penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah Provinsi terdiri atas Gubernur dibantu oleh PD pelaksana Urusan Pemerintahan Bidang Persandian.

Pasal 6

- (1) Gubernur memimpin dan bertanggung jawab atas penyelenggaraan Persandian yang menjadi kewenangan Provinsi.
- (2) PD pelaksana Urusan Pemerintahan Bidang Persandian bertanggung jawab atas kinerja pelaksanaan Urusan Pemerintahan bidang Persandian sesuai dengan tugas dan fungsinya.

Pasal 7

- (1) PD pelaksana Urusan Pemerintahan bidang Persandian 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 perencanaan pembangunan daerah sebagaimana dimaksud pada ayat (3) berupa rencana pembangunan jangka panjang daerah, rencana pembangunan jangka menengah daerah, dan rencana kerja Pemerintah Provinsi.

Pasal 8

- (1) Dalam rangka menjabarkan rencana pembangunan jangka menengah daerah sebagaimana dimaksud dalam Pasal 7 ayat (4), PD pelaksana Urusan Pemerintahan Bidang Persandian menyusun rencana strategis PD yang memuat tujuan, sasaran, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintahan Daerah Provinsi.
- (2) Dalam rangka menjabarkan rencana kerja Pemerintah Daerah Provinsi sebagaimana dimaksud dalam Pasal 7 ayat (4), PD pelaksana Urusan Pemerintahan Bidang Persandian menyusun rencana kerja Perangkat Daerah 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 lingkungan Pemerintah Daerah Provinsi.

BAB II

PENGELOLAAN DAN PERLINDUNGAN INFORMASI

Bagian Kesatu

Pengelolaan Informasi Berklasifikasi

Pasal 9

- (1) Pengelolaan Informasi Berklasifikasi di lingkungan Pemerintah Provinsi harus menggunakan pengamanan Informasi.
- (2) Pengelolaan Informasi Berklasifikasi sebagaimana dimaksud ayat (1) terdiri dari:
 - a. pembuatan;
 - b. pemberian label;
 - c. pengiriman dan penerimaan; dan
 - d. penyimpanan.

Paragraf 1
Pembuatan Informasi Berklasifikasi

Pasal 10

- (1) Pembuatan Informasi Berklasifikasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a dilakukan oleh pemilik Informasi atau pengelola Informasi;
- (2) Pembuatan Informasi Berklasifikasi harus menggunakan sarana dan prasarana milik dinas yang hanya dimanfaatkan untuk kepentingan dinas;
- (3) Sarana dan prasarana sebagaimana dimaksud ayat (2) harus memiliki kriteria aman secara fisik, administrasi, dan lojik;
- (4) Konsep Informasi Berklasifikasi tidak boleh disimpan dan harus dihancurkan baik dalam bentuk tercetak maupun elektronik;
- (5) Dokumen elektronik yang berisi Informasi Berklasifikasi yang telah disahkan harus disimpan dalam bentuk yang tidak bisa diubah atau dimodifikasi dengan menggunakan Tanda Tangan Elektronik; dan
- (6) Penggandaan dan/atau perubahan Informasi Berklasifikasi harus mendapat persetujuan dari pemilik Informasi.

Paragraf 2
Pemberian Label Informasi Berklasifikasi

Pasal 11

- (1) Pemberian label sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b dilakukan pada Informasi Berklasifikasi yang telah disahkan dan media penyimpanannya sesuai dengan Tingkat Kerahasiaan Informasinya.
- (2) Tingkat Kerahasiaan Informasi sebagaimana dimaksud pada ayat (1) di suatu PD harus diperlakukan sama tingkat kerahasiaannya oleh PD lainnya.
- (3) Tingkat Kerahasiaan Informasi sebagaimana dimaksud pada ayat (1) diklasifikasikan dalam 3 (tiga) tingkatan, yaitu:
 - a. terbatas;
 - b. rahasia; dan
 - c. sangat rahasia.

Pasal 12

Label sebagaimana dimaksud dalam Pasal 11 diberikan dengan ketentuan:

- a. Dokumen cetak:
 - 1. Label 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. Label ditulis pada baris subjek pada header surat elektronik;
- c. Label diberikan dalam metadata Dokumen Elektronik pada header atau footer atau menggunakan watermark di setiap halaman termasuk cover;
- d. Label diberikan dalam metadata sistem/aplikasi pada basis data dan aplikasi; dan/atau
- e. Media penyimpanan lain:
 - 1. label ditempelkan pada fisik media penyimpanan;
 - 2. label 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 dan Penerimaan Informasi Berklasifikasi

Pasal 13

- (1) Pengiriman dan penerimaan Dokumen Elektronik yang berisi Informasi Berklasifikasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c harus menggunakan Persandian dan dikirim melalui jalur komunikasi yang aman.
- (2) Pengiriman dokumen cetak yang berisi Informasi Berklasifikasi menggunakan pengamanan fisik berlapis dengan memasukkannya ke dalam dua amplop, yaitu:
 - a. amplop pertama dibubuhi alamat lengkap, nomor, cap dinas, dan cap yang sesuai dengan klasifikasi dan derajat kecepatan (kilat, sangat segera, segera, dan biasa); dan
 - b. amplop pertama sebagaimana dimaksud pada angka 1 dimasukkan ke dalam amplop kedua dengan tanda yang sama kecuali cap klasifikasi.
- (3) Pengiriman dokumen cetak yang berisi Informasi Berklasifikasi sebagaimana dimaksud ayat (2) harus tercatat dalam buku ekspedisi sebagai bukti pengiriman atau dibuatkan tanda bukti pengiriman tersendiri.

Paragraf 4
Penyimpanan Informasi Berklasifikasi

Pasal 14

Penyimpanan Informasi Berklasifikasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf d disimpan dalam bentuk Dokumen Elektronik dan/atau dokumen cetak.

Pasal 15

Penyimpanan Informasi Berklasifikasi 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, perangkat *mobile*, atau media penyimpanan pribadi;
- d. melakukan perekaman data (*backup*) secara berkala; dan
- e. media penyimpanan dilarang digunakan, dipinjam, atau dibawa keluar ruangan atau keluar kantor tanpa izin pengelola Informasi.

Pasal 16

Penyimpanan Informasi Berklasifikasi 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 Kedua
Perlindungan Informasi Berklasifikasi

Pasal 17

Perlindungan Informasi Berklasifikasi di lingkungan Pemerintah Provinsi dan Kabupaten meliputi:

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

Paragraf 1
Perlindungan Fisik

Pasal 18

- (1) Perlindungan fisik sebagaimana dimaksud dalam Pasal 17 huruf a dilakukan untuk melindungi keberadaan dan fungsi sarana fisik komunikasi serta segala kegiatan yang berlangsung di dalamnya dari ancaman dan gangguan seperti pencurian, kerusakan, dan radiasi gelombang elektromagnetik.
- (2) Perlindungan fisik sebagaimana dimaksud dalam Pasal 17 huruf a dilakukan melalui:
 - a. kendali akses ruang;
 - b. pemasangan teralis;
 - c. penggunaan kunci ganda;
 - d. pemasangan CCTV; dan/atau
 - e. penggunaan ruang TEMPEST.

Paragraf 2
Perlindungan Administrasi

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) dituangkan dalam bentuk peraturan tertulis yang menerangkan kebijakan, standar, dan prosedur operasional dalam pengamanan Informasi Berklasifikasi.

Paragraf 3
Perlindungan Logik

Pasal 20

- (1) Perlindungan logik sebagaimana dimaksud dalam Pasal 17 huruf c dilakukan dengan menggunakan perlindungan logik menggunakan teknik Kriptografi dan steganografi untuk memenuhi aspek: kerahasiaan, keutuhan, otentikasi, dan nir penyangkalan.
- (2) Perlindungan logik yang menggunakan teknik Kriptografi dan steganografi sebagaimana dimaksud pada ayat (2) harus memenuhi standar dan direkomendasikan oleh Badan Siber dan Sandi Negara.

Bagian Ketiga
Pengelolaan dan Perlindungan Informasi Publik

Pasal 21

- (1) Pengelolaan dan perlindungan Informasi Publik di Pemerintah Provinsi meliputi:
 - a. pengiriman Informasi yang terbuka melalui jaringan yang aman.
 - b. pengamanan transaksi elektronik melalui implementasi Sertifikat Elektronik.
- (2) Implementasi Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) huruf b bertujuan untuk menjamin keutuhan, autentikasi dan nir-penyangkalan dokumen elektronik.

BAB III

PENGELOLAAN SUMBER DAYA PERSANDIAN

Pasal 22

- (1) PD pelaksana Urusan Pemerintah Bidang Persandian harus melakukan pengelolaan sumber daya Persandian.
- (2) Pengelolaan sumber daya Persandian sebagaimana dimaksud dalam ayat (1), terdiri dari:
 - a. pengelolaan sumber daya manusia; dan
 - b. pengelolaan sarana dan prasarana.

Bagian Kesatu

Pengelolaan Sumber Daya Manusia

Pasal 23

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam pasal 22 ayat (2) huruf a meliputi perencanaan dan pengembangan sumber daya manusia.
- (2) Dalam hal pengelolaan sumber daya manusia sebagaimana pada pasal ayat (1), Pemerintah Provinsi 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 24

Perencanaan sumber daya manusia sebagaimana dimaksud dalam pasal 23 ayat (1) disusun dengan ketentuan:

- a. memperhatikan jumlah dan kompetensi yang dibutuhkan sesuai dengan hasil analisis beban kerja serta formasi jabatan;
- b. memperhatikan standar kompetensi yang telah ditetapkan oleh Badan Siber dan Sandi Negara;
- c. mengusulkan kebutuhan sumber daya manusia kepada Badan Kepegawaian Daerah.

Pasal 25

- (1) Pengembangan sumber daya manusia sebagaimana dimaksud dalam pasal 23 ayat (1) dilakukan melalui:
 - a. pendidikan dan pelatihan Fungsional Sandiman;
 - b. pendidikan dan pelatihan teknis sandi;
 - c. bimbingan teknis; dan
 - d. kegiatan pengembangan kompetensi lain yang terkait dengan Persandian dan teknologi informasi serta bidang ilmu lainnya yang dibutuhkan.
- (2) Pengembangan sumber daya manusia sebagaimana dimaksud dalam ayat (1) merupakan pengembangan sumber daya manusia yang terkait dengan ilmu Persandian dan teknologi Informasi serta bidang ilmu lainnya yang dibutuhkan.

Pasal 26

Sumber daya manusia yang sudah tidak melaksanakan tugas pada PD pelaksana Urusan Pemerintah Bidang Persandian harus disesuaikan kewenangannya, yaitu:

- a. pencabutan atau pemutusan hak akses terhadap Informasi dan fasilitas pemroses Informasi Berklasifikasi; dan
- b. pelaksanaan prosedur pengamanan (serah terima) materiil sandi.

Bagian Kedua Pengelolaan Sarana dan Prasarana

Pasal 27

- (1) Pengelolaan sarana dan prasarana Persandian sebagaimana dimaksud dalam pasal 22 ayat (2) huruf b meliputi:

- a. materiil sandi;
 - b. tempat kegiatan sandi; dan
 - c. alat pendukung utama (APU) Persandian.
- (2) Pengelolaan sarana dan prasarana Persandian dilaksanakan oleh Aparatur Sipil Negara Pemerintah Provinsi yang berada pada bidang atau seksi penyelenggara Persandian pada PD pelaksana Urusan Pemerintahan Bidang Persandian.
- (3) Ketentuan mengenai pengelolaan sarana dan prasarana mengacu pada Peraturan Kepala Badan Siber dan Sandi Negara.

Pasal 28

Pengelolaan materiil sandi yang dilaksanakan oleh Pemerintah Provinsi sebagaimana dimaksud dalam pasal 27 ayat (1) huruf a yaitu pengelolaan peralatan sandi.

Pasal 29

Pengelolaan peralatan sandi yang dilaksanakan oleh Pemerintah Provinsi dan sebagaimana dimaksud dalam pasal 28 huruf a adalah:

- a. perencanaan kebutuhan;
- b. penggunaan;
- c. pemeliharaan;
- d. perbaikan;
- e. pendistribusian; dan
- f. pengawasan dan pengendalian.

Paragraf 1

Perencanaan Kebutuhan Peralatan Sandi

Pasal 30

- (1) Pemerintah Provinsi merumuskan rencana kebutuhan peralatan sandi dan menetapkannya sebagai peralatan sandi kebutuhan Pemerintah Provinsi.
- (2) Perumusan rencana kebutuhan peralatan sandi harus berdasarkan pada peralatan sandi yang telah direkomendasikan oleh Badan Siber dan Sandi Negara.
- (3) Hasil penetapan peralatan sandi diajukan Pemerintah Provinsi kepada Badan Siber dan Sandi Negara untuk permohonan pemenuhan peralatan sandi kebutuhan Pemerintah Provinsi.

Paragraf 2
Penggunaan Peralatan Sandi

Pasal 31

- (1) Peralatan sandi digunakan untuk kepentingan pengamanan Informasi.
- (2) Penggunaan peralatan sandi dilaksanakan menurut peraturan perundang-undangan.

Paragraf 3
Pemeliharaan Peralatan Sandi

Pasal 32

- (1) Pemeliharaan peralatan sandi dilakukan berdasarkan prinsip kehati-hatian dan ketepatan.
- (2) Pemeliharaan peralatan sandi yang dilakukan Pemerintah Provinsi mencakup:
 - a. memastikan peralatan sandi bebas dari debu/kotoran atau benda lain yang memicu gangguan operasional peralatan sandi;
 - b. menjaga ketersediaan dan kestabilan arus listrik sesuai persyaratan pada peralatan sandi;
 - c. menjaga dan memonitor ketersediaan koneksi saluran telekomunikasi pada peralatan sandi;
 - d. memastikan peralatan sandi dapat berfungsi sebagaimana mestinya;
 - e. menjaga kestabilan suhu ruangan tempat peletakkan Peralatan sandi;
 - f. meletakkan peralatan sandi pada tempat yang aman dari kemungkinan bencana, pencurian, dan kehilangan.
 - g. memastikan kelengkapan perangkat; dan
 - h. memastikan kelengkapan dokumen serah terima barang, berita acara serah terima dan/atau penarikan.
- (3) Kegiatan pemasangan kunci sistem sandi ke dalam peralatan sandi harus dilakukan oleh Aparatur Sipil Negara berkualifikasi sandi yang bertugas secara penuh di bidang persandian.
- (4) Kunci sistem sandi yang diterima Pemerintah Provinsi tidak boleh diubah atau digandakan.
- (5) Kunci sistem sandi harus disimpan pada tempat yang aman dan kuat dalam brankas atau *strong room* atau lemari besi dengan perkuatan kunci kombinasi.

- (6) Jangka waktu penyimpanan kunci sistem sandi dilakukan sampai dengan pelaksanaan pemusnahan.
- (7) Pemeliharaan dan perawatan kunci sistem sandi merupakan kegiatan merawat kunci sistem sandi agar mutu kunci sistem sandi tetap terjaga dan/atau tidak mengalami kerusakan.

Paragraf 4
Perbaikan Peralatan Sandi

Pasal 33

- (1) Kategori perbaikan peralatan sandi meliputi:
 - a. perbaikan umum; dan
 - b. perbaikan khusus.
- (2) Perbaikan umum sebagaimana dimaksud dalam ayat (1) huruf a, merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis.
- (3) Perbaikan khusus sebagaimana dimaksud dalam ayat (2) huruf b, merupakan perbaikan yang berkaitan dengan aspek kriptografis.

Pasal 34

- (1) Perbaikan peralatan sandi yang dilakukan oleh Pemerintah Provinsi adalah perbaikan umum.
- (2) Dalam hal melakukan perbaikan umum peralatan sandi, Pemerintah Provinsi mengirimkan surat pemberitahuan kerusakan yang ditujukan kepada Kepala Badan Siber dan Sandi Negara.
- (3) Surat pemberitahuan kerusakan sebagaimana dimaksud pada Ayat (2), memuat keterangan mengenai nama peralatan sandi, nomor seri, deskripsi kerusakan dan pernyataan untuk diperbaiki.
- (4) Dalam hal Pemerintah Provinsi tidak dapat melaksanakan perbaikan umum peralatan sandi, Pemerintah Provinsi mengajukan surat permohonan perbaikan peralatan sandi kepada Badan Siber dan Sandi Negara.

Pasal 35

- (1) Dalam hal perbaikan khusus peralatan sandi, Pemerintah Provinsi mengirimkan surat permohonan perbaikan yang ditujukan kepada Kepala Badan Siber dan Sandi Negara.

- (2) Surat pemberitahuan kerusakan sebagaimana dimaksud pada ayat (1), memuat keterangan mengenai nama peralatan sandi, nomor seri, deskripsi kerusakan dan pernyataan untuk diperbaiki.

Paragraf 5
Pendistribusian Peralatan Sandi

Pasal 36

Pendistribusian peralatan sandi kepada PD dan/atau pejabat/pimpinan Pemerintah Provinsi wajib memperhatikan ketentuan sebagai berikut:

- a. dilengkapi dengan berita acara penyerahan;
- b. terjamin keamanan dan keutuhannya sehingga terhindar dari kehilangan dan kerusakan; dan
- c. dalam keadaan netral atau non aktif (tidak terisi kunci sistem sandi).

Paragraf 5
Pengawasan dan Pengendalian

Pasal 37

- (1) Pengawasan dan pengendalian peralatan sandi harus dilakukan secara menyeluruh, terus menerus dan berkesinambungan.
- (2) Pemerintah Provinsi harus membuat laporan rutin dan/atau sewaktu-waktu tentang pelaksanaan pengawasan dan pengendalian peralatan sandi berdasarkan kewenangan dan tanggungjawab masing-masing.

Pasal 38

Tempat kegiatan sandi Pemerintah Provinsi harus mengikuti standar tempat kegiatan sandi yang diatur oleh ketentuan Badan Siber dan Sandi Negara.

Pasal 39

Pengelolaan APU Persandian yang dilaksanakan oleh Pemerintah Provinsi sebagaimana dimaksud dalam 27 ayat (1) huruf c adalah:

- a. pemeliharaan; dan
- b. perbaikan.

Pasal 40

- (1) Pemeliharaan APU Persandian dilakukan berdasarkan prinsip kehati-hatian dan ketepatan.
- (2) Pemeliharaan APU Persandian yang dilakukan Pemerintah Provinsi mencakup:
 - a. memastikan peralatan sandi bebas dari debu/kotoran atau benda lain yang memicu gangguan operasional Peralatan sandi;
 - b. menjaga ketersediaan dan kestabilan arus listrik sesuai persyaratan pada peralatan sandi;
 - c. menjaga dan memonitor ketersediaan koneksi saluran telekomunikasi pada Peralatan sandi;
 - d. memastikan peralatan sandi dapat berfungsi sebagaimana mestinya;
 - e. menjaga kestabilan suhu ruangan tempat peletakkan Peralatan sandi;
 - f. meletakkan peralatan sandi pada tempat yang aman dari kemungkinan bencana, pencurian, dan kehilangan.
 - g. memastikan kelengkapan perangkat;
 - h. memastikan kelengkapan dokumen serah terima barang, berita acara serah terima dan/atau penarikan.

Pasal 41

- (1) Perbaikan APU Persandian hanya meliputi perbaikan yang bersifat umum.
- (2) Perbaikan umum sebagaimana dimaksud dalam ayat (1), merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis.
- (3) Dalam hal melakukan perbaikan umum APU Persandian, Pemerintah Provinsi mengirimkan surat pemberitahuan kerusakan yang ditujukan kepada Kepala Badan Siber dan Sandi Negara.
- (4) Surat pemberitahuan kerusakan sebagaimana dimaksud pada ayat (3), memuat keterangan mengenai nama peralatan sandi, nomor seri, deskripsi kerusakan dan pernyataan untuk diperbaiki.
- (5) Dalam hal Pemerintah Provinsi tidak dapat melaksanakan perbaikan umum terhadap APU, Pemerintah Provinsi mengajukan surat permohonan perbaikan peralatan sandi kepada Badan Siber dan Sandi Negara.

BAB IV
POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 42

- (1) Penyelenggaraan JKS untuk pengamanan informasi berklasifikasi di Pemerintah Provinsi diterapkan melalui penetapan pola hubungan komunikasi sandi.
- (2) Untuk JKS di lingkungan Pemerintah Kabupaten/Kota mengacu pada peraturan perundang-undangan.

Pasal 43

Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud dalam pasal 42 dilakukan melalui tahapan:

- a. identifikasi;
- b. analisis; dan
- c. penetapan hasil.

Pasal 44

Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud dalam pasal 43 huruf a, meliputi:

- a. identifikasi pola hubungan komunikasi pejabat/pimpinan di Pemerintah Provinsi yang sedang dilaksanakan;
- b. identifikasi alur Informasi yang dikomunikasikan antar PD;
- c. identifikasi dan/atau penyediaan sarana dan prasarana teknologi Informasi dan komunikasi yang digunakan oleh pejabat/pimpinan di Pemerintah Provinsi;
- d. infrastruktur komunikasi yang ada di wilayah Pemerintah Provinsi; dan
- e. kompetensi personil yang dibutuhkan.

Pasal 45

- (1) Analisis pola hubungan komunikasi sandi yang diperlukan sebagaimana dimaksud dalam Pasal 43 huruf b dilakukan berdasarkan hasil identifikasi pola hubungan komunikasi, meliputi:
 - a. identifikasi pengelola layanan penyelenggaraan persandian;
 - b. identifikasi sarana dan prasarana; dan
 - c. identifikasi pembiayaan.

- (2) Identifikasi pengelola layanan penyelenggaraan persandian sebagaimana dimaksud pada ayat (1) huruf a yaitu kegiatan untuk mengidentifikasi personil dan kompetensi yang dibutuhkan dalam menyelenggarakan kegiatan Persandian.
- (3) Identifikasi sarana dan prasarana sebagaimana dimaksud pada ayat (1) huruf b, meliputi:
 - a. materiil sandi;
 - b. jaringan komunikasi sandi;
 - c. alat pendukung utama (APU) persandian;
 - d. tempat kegiatan sandi; dan
 - e. sarana penunjang.
- (4) Identifikasi pembiayaan sebagaimana dimaksud pada ayat (1) huruf c meliputi identifikasi anggaran yang dibutuhkan oleh penyelenggara Persandian di Pemerintah Provinsi dalam periode waktu satu tahun anggaran.

Pasal 46

- (1) Identifikasi materiil sandi sebagaimana dimaksud dalam pasal 45 ayat (3) huruf a meliputi identifikasi terhadap kebutuhan peralatan sandi dan kunci sistem sandi yang didasarkan pada kondisi infrastuktur, jenis komunikasi, dan hierarki komunikasinya.
- (2) Identifikasi jaringan komunikasi sandi sebagaimana dimaksud dalam pasal 45 ayat (3) huruf b meliputi identifikasi terhadap:
 - a. PD yang akan terhubung dalam jaringan komunikasi sandi termasuk di dalamnya unit kerja dalam Pemerintah Provinsi yang akan mengoperasikan peralatan sandi;
 - b. Pejabat Pemerintah Provinsi yang akan terhubung dalam jaringan komunikasi sandi termasuk di dalamnya penentuan hierarki komunikasi; dan
 - c. Infrastruktur komunikasi yang ada di lingkungan Pemerintah Provinsi dan Kabupaten/Kota.
- (3) Identifikasi APU Persandian sebagaimana dimaksud dalam pasal 45 ayat (3) huruf c meliputi identifikasi kebutuhan terhadap perangkat yang mendukung penyelenggaraan Persandian.
- (4) Identifikasi tempat kegiatan sandi sebagaimana dimaksud dalam pasal 45 ayat (3) huruf d meliputi identifikasi kebutuhan pengamanan terhadap tempat yang digunakan untuk operasional Persandian sesuai dengan jenis komunikasinya.

- (5) Identifikasi sarana penunjang sebagaimana dimaksud dalam pasal 45 ayat (3) huruf e meliputi identifikasi kebutuhan terhadap peralatan yang mendukung dalam kegiatan penyelenggaraan Persandian, meliputi alat tulis kantor dan sarana pengolah data.

Pasal 47

PD pelaksana Urusan Pemerintahan Bidang Persandian mengoordinasikan hasil identifikasi dan analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 44 dan Pasal 45 secara berjenjang sampai ke Badan Siber dan Sandi Negara untuk melihat dan menjamin keterhubungan (interkoneksi) secara vertikal.

Pasal 48

- (1) Hasil identifikasi dan analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam pasal 43 ditetapkan dengan Keputusan Gubernur.
- (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 49

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

BAB V OPERASIONAL DUKUNGAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Pasal 50

- (1) Operasional dukungan Persandian untuk pengamanan Informasi merupakan kegiatan operasional yang tidak terkait dengan Kriptografi namun mendukung terciptanya keamanan Informasi.
- (2) Operasional dukungan Persandian untuk pengamanan Informasi sebagaimana dimaksud ayat (1) meliputi:

- a. Pengamanan gelombang frekuensi (jamming);
 - b. Kontra penginderaan; dan
 - c. Penilaian keamanan sistem Informasi.
- (3) Pelaksana kegiatan operasional dukungan Persandian untuk pengamanan Informasi ialah aparatur sipil negara di Pemerintah Provinsi yang berada pada Bidang atau Seksi penyelenggara Persandian pada PD pelaksana Urusan Pemerintahan Bidang Persandian.
- (4) Pelaksanaan operasional dukungan Persandian untuk pengamanan Informasi Pemerintah Provinsi mengacu pada ketentuan peraturan perundang-undangan.

Pasal 51

- (1) Pengamanan gelombang frekuensi (jamming) sebagaimana dimaksud dalam Pasal 50 ayat (2) huruf a merupakan upaya pengamanan sinyal dari ancaman penyalahgunaan sinyal untuk kepentingan yang tidak bertanggung jawab dengan cara menutup/memutus frekuensi.
- (2) Pengamanan gelombang frekuensi (jamming) dilakukan berdasarkan hasil identifikasi pada kegiatan Pemerintah Provinsi yang berpotensi timbulnya ancaman penyalahgunaan sinyal.

Pasal 52

- (1) Kontra penginderaan sebagaimana dimaksud dalam Pasal 50 ayat (2) huruf b merupakan upaya melakukan deteksi dari pengawasan oleh pihak yang tidak berwenang pada objek ruang tertentu.
- (2) Kontra penginderaan sebagaimana dimaksud pada ayat (1) dilakukan pada objek ruang milik Pemerintah Provinsi yang digunakan untuk melakukan komunikasi terkait Informasi Berklasifikasi.

Pasal 53

Pelaksanaan kontra penginderaan sebagaimana dimaksud dalam Pasal 52 dilakukan secara berkala.

Pasal 54

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

- (2) Hasil pelaksanaan kontra penginderaan harus ditindaklanjuti oleh Pemerintah Provinsi sebagai bahan evaluasi dan perbaikan penyelenggaraan Urusan Pemerintahan Bidang Persandian.

Pasal 55

- (1) Penilaian keamanan sistem Informasi sebagaimana dimaksud dalam Pasal 50 ayat 2 huruf c merupakan upaya untuk mengukur tingkat kerawanan dan keamanan dari sistem Informasi di Pemerintah Provinsi.
- (2) Penilaian keamanan sistem Informasi dilakukan pada sistem Informasi milik Pemerintah Provinsi.

Pasal 56

- (1) Pemerintah Provinsi melakukan kegiatan penilaian keamanan sistem Informasi secara mandiri.
- (2) Dalam hal Pemerintah Provinsi tidak dapat melakukan kegiatan penilaian keamanan sistem Informasi secara mandiri sebagaimana dimaksud pada ayat (1), Pemerintah Provinsi mengajukan permohonan penilaian keamanan sistem Informasi kepada Badan Siber dan Sandi Negara.

Pasal 57

Hasil pelaksanaan Penilaian keamanan sistem Informasi sebagaimana dimaksud pada Pasal 56 harus ditindaklanjuti oleh Pemerintah Provinsi sebagai bahan evaluasi dan perbaikan penyelenggaraan Urusan Pemerintahan Bidang Persandian.

BAB VI LAYANAN SERTIFIKAT ELEKTRONIK

Pasal 58

Layanan Sertifikat Elektronik di Pemerintah Provinsi bertujuan untuk menjamin keutuhan, otentikasi dan nir penyangkalan Dokumen Elektronik.

Pasal 59

- (1) Layanan Sertifikat Elektronik dapat dimanfaatkan oleh Pemerintah Provinsi jika telah memenuhi persyaratan dan telah diberikan kewenangan oleh Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara sesuai ketentuan peraturan perundang-undangan.
- (2) Setiap aparatur sipil negara Pemerintah Provinsi dapat memiliki Sertifikat Elektronik yang digunakan selama melaksanakan tugas kedinasan.
- (3) Kepemilikan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) difasilitasi oleh PD pelaksana Urusan Pemerintahan Bidang Persandian.

Pasal 60

Tugas kedinasan sebagaimana dimaksud dalam Pasal 59 ayat (2) meliputi:

- a. pengiriman dan pembuatan surat elektronik (email);
- b. pembuatan dokumen persuratan elektronik; dan/atau
- c. pembuatan Dokumen Elektronik lainnya yang menggunakan aplikasi dan sistem elektronik.

Pasal 61

Aplikasi dan Sistem Elektronik yang dimiliki oleh Pemerintah Provinsi harus memanfaatkan layanan Sertifikat Elektronik dalam rangka pengamanan Informasi.

Pasal 62

- (1) Proses pemanfaatan Layanan Sertifikat Elektronik dilakukan melalui:
 - a. pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan Sertifikat Elektronik;
 - b. pengembangan aplikasi pendukung penggunaan Sertifikat Elektronik;
 - c. fasilitasi kegiatan sosialisasi dan bimbingan teknis terkait Sertifikat Elektronik; dan
 - d. pengawasan dan evaluasi penggunaan Sertifikat Elektronik.
- (2) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) huruf a, meliputi:
 - a. menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi, dan rekomendasi dari instansi;

- b. menyetujui /menolak permintaan pendaftaran Sertifikat Elektronik;
- c. menindaklanjuti permintaan Sertifikat Elektronik kepada BSR E;
- d. menyampaikan Sertifikat Elektronik kepada pemohon; dan
- e. melakukan pengarsipan berkas pendaftaran Sertifikat Elektronik (hardcopy & softcopy).

BAB VII PEMANTAUAN DAN EVALUASI

Pasal 63

Pemantauan dan evaluasi penyelenggaraan Persandian merupakan upaya untuk memantau perkembangan, mengidentifikasi hambatan, dan upaya perbaikan dalam penyelenggaraan Persandian untuk pengamanan Informasi di Pemerintah Provinsi.

Pasal 64

- (1) Pemantauan dan evaluasi penyelenggaraan Persandian di Pemerintah Provinsi sebagaimana dimaksud dalam Pasal 63 dilaksanakan oleh PD pelaksana Urusan Pemerintahan bidang Persandian meningkatkan kinerja Persandian.
- (2) Pemantauan dan evaluasi harus ditindaklanjuti dengan rencana perbaikan sebagai bahan masukan bagi penyusunan kebijakan, program, dan kegiatan penyelenggaraan Persandian tahun berikutnya.

Pasal 65

Pemantauan dan evaluasi penyelenggaraan Persandian sebagaimana dimaksud dalam Pasal 63 meliputi:

- a. pengawasan dan evaluasi yang bersifat rutin dan sewaktu-waktu; dan
- b. pengawasan dan evaluasi yang bersifat tahunan.

Pasal 66

Pemantauan dan evaluasi yang bersifat rutin dan sewaktu-waktu sebagaimana dimaksud dalam Pasal 65 huruf a terdiri dari:

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

Pasal 67

Pemantauan dan evaluasi yang bersifat tahunan sebagaimana dimaksud dalam Pasal 65 huruf b terdiri dari:

- a. pengukuran tingkat pemanfaatan layanan Persandian oleh PD di Pemerintah Provinsi;
- b. penilaian mandiri terhadap penyelenggaraan Persandian di Pemerintah Provinsi;
- c. pengukuran tingkat kepuasan PD di Pemerintah Provinsi terhadap layanan Persandian yang dikelola oleh PD pelaksana Urusan Pemerintahan Bidang Persandian; dan
- d. penyusunan Laporan Penyelenggaraan Persandian Tahunan Pemerintah Provinsi.

BAB VIII

KOORDINASI DAN KONSULTASI

Pasal 68

Dalam rangka pelaksanaan Urusan Pemerintahan Bidang Persandian, PD pelaksana Urusan Pemerintahan Bidang Persandian di Pemerintah Provinsi dapat melaksanakan koordinasi dan/atau konsultasi ke Badan Siber dan Sandi Negara, PD terkait maupun antar Pemerintah Daerah lainnya.

BAB IX

PELAPORAN

Pasal 69

- (1) Laporan hasil evaluasi penyelenggaraan Persandian untuk pengamanan informasi Pemerintah Provinsi disampaikan oleh Gubernur 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, Gubernur dapat menyampaikan laporan langsung kepada Kepala Badan Siber dan Sandi Negara.

**BAB X
PEMBIAYAAN**

Pasal 70

Pembiayaan penyelenggaraan Persandian untuk pengamanan Informasi di Pemerintah Provinsi bersumber dari anggaran, pendapatan dan belanja daerah Provinsi.

**BAB XI
KETENTUAN PENUTUP**

Pasal 71

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Kalimantan Tengah.

Ditetapkan di Palangka Raya
pada tanggal 24 April 2018

GUBERNUR KALIMANTAN TENGAH,

ttd

SUGIANTO SABRAN

Diundangkan di Palangka Raya
pada tanggal 24 April 2018

**Plt. SEKRETARIS DAERAH
PROVINSI KALIMANTAN TENGAH,**

ttd

FAHRIZAL FITRI

BERITA DAERAH PROVINSI KALIMANTAN TENGAH TAHUN 2018 NOMOR 11

Salinan sesuai dengan aslinya

KEPALA BIRO HUKUM,

ttd

**HASANUDIN
NIP. 19580614 197901 1 001**