



BERITA NEGARA REPUBLIK INDONESIA

No.1054, 2019

BSSN. Persandian. Pengamanan Informasi.
Pemerintah Daerah. Pelaksanaan.

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2019
TENTANG
PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

- Menimbang :
- a. bahwa untuk melaksanakan urusan pemerintahan bidang persandian di daerah diperlukan norma, standar, prosedur, dan kriteria;
 - b. bahwa berdasarkan ketentuan Pasal 16 ayat (1) huruf a Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah 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, Badan Siber dan Sandi Negara berwenang untuk menetapkan norma, standar, prosedur, dan kriteria;
 - c. bahwa Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintahan Daerah Provinsi dan Kabupaten/Kota dinilai sudah tidak relevan dengan dinamika perubahan peraturan perundang-undangan sehingga perlu diganti;
 - d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu

menetapkan Peraturan Badan Siber dan Sandi Negara tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;

- Mengingat :
1. 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);
 2. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100), sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Republik Indonesia Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 277);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI PEMERINTAH DAERAH.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Pemerintah Pusat adalah Presiden Republik Indonesia yang memegang kekuasaan pemerintahan negara Republik Indonesia yang dibantu oleh Wakil Presiden dan menteri sebagaimana dimaksud dalam Undang-Undang

Dasar Negara Republik Indonesia Tahun 1945.

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. Perangkat Daerah pelaksana urusan pemerintahan bidang Persandian selanjutnya disebut Perangkat Daerah adalah unsur pembantu kepala daerah dalam penyelenggaraan urusan pemerintahan bidang persandian.
4. 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.
5. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
6. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
7. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
8. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
9. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang

Persandian dan yang memiliki nilai manfaat.

10. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
11. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Pasal 2

Pelaksanaan persandian untuk pengamanan informasi di pemerintah daerah bertujuan untuk:

- a. menciptakan harmonisasi dalam melaksanakan Persandian untuk pengamanan informasi antara Pemerintah Pusat dan pemerintah daerah;
- b. meningkatkan komitmen, efektivitas, dan kinerja pemerintah daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi; dan
- c. memberikan pedoman bagi pemerintah daerah dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah.

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi di pemerintah daerah sebagaimana dimaksud dalam Pasal 2 meliputi:

- a. penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah provinsi dan kabupaten/kota; dan
- b. penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota.

BAB II
PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI PEMERINTAH
DAERAH PROVINSI DAN KABUPATEN/KOTA

Bagian Kesatu
Umum

Pasal 4

- (1) Penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah provinsi dan kabupaten/kota sebagaimana dimaksud dalam Pasal 3 huruf a dilaksanakan melalui:
 - a. penyusunan kebijakan Pengamanan Informasi;
 - b. pengelolaan sumber daya Keamanan Informasi;
 - c. pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik; dan
 - d. penyediaan layanan Keamanan Informasi.
- (2) Gubernur atau Bupati/Wali Kota sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1).

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 5

- Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a dilakukan dengan:
- a. menyusun rencana strategis Pengamanan Informasi;
 - b. menetapkan arsitektur Keamanan Informasi; dan
 - c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 6

- (1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf a disusun oleh Gubernur atau Bupati/Wali Kota sesuai dengan kewenangannya.
- (2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Perangkat Daerah.
- (3) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
 - b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.
- (4) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
- (5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Gubernur atau Bupati/Wali Kota dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (6) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (5) Gubernur atau Bupati/Wali Kota dapat menunjuk Perangkat Daerah.

Pasal 7

- (1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf b ditetapkan oleh Gubernur atau Bupati/Wali Kota sesuai dengan kewenangannya.
- (2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
 - a. infrastruktur teknologi informasi;
 - b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan

- c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
- (3) Dalam melakukan penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) Gubernur atau Bupati/Wali Kota dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Gubernur atau Bupati/Wali Kota dapat menunjuk Perangkat Daerah.
- (5) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
- (6) Arsitektur Keamanan Informasi dilakukan evaluasi oleh Gubernur atau Bupati/Wali Kota pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 8

- (1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf c ditetapkan oleh Gubernur atau Bupati/Wali Kota sesuai dengan kewenangannya.
- (2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
 - a. keamanan sumber daya teknologi informasi;
 - b. keamanan akses kontrol;
 - c. keamanan data dan informasi;
 - d. keamanan sumber daya manusia;
 - e. keamanan jaringan;
 - f. keamanan surat elektronik;
 - g. keamanan pusat data; dan/atau
 - h. keamanan komunikasi.
- (3) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Gubernur atau Bupati/Wali Kota dapat melakukan koordinasi dan konsultasi kepada BSSN.

- (4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Gubernur atau Bupati/Wali Kota dapat menunjuk Perangkat Daerah.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 9

- (1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b dilaksanakan oleh Perangkat Daerah.
- (2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
 - b. pengelolaan sumber daya manusia; dan
 - c. manajemen pengetahuan.

Pasal 10

- (1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
- (2) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 11

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b dilakukan oleh Perangkat Daerah.

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

Pasal 12

- (1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dilaksanakan dengan ketentuan:
- a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjurangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop*, seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;
 - b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau pemerintah daerah masing-masing; dan
 - c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.
- (2) Pembinaan karir sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b dilaksanakan dengan ketentuan:
- a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
 - b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.
- (3) Pendayagunaan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

Pasal 13

- (1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c dilakukan oleh Perangkat Daerah.
- (2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
- (3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi pemerintah daerah.
- (4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah.
- (5) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah berkoordinasi dan dapat melakukan konsultasi dengan BSSN.
- (6) Ketentuan lebih lanjut mengenai pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah diatur dengan Peraturan Badan.

Bagian Keempat

Pengamanan Sistem Elektronik dan
Pengamanan Informasi Nonelektronik

Pasal 14

Pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c dilaksanakan oleh Perangkat Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 14 terdiri atas:

- a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data dan informasi;

- b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
- c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 16

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 Perangkat Daerah melakukan:
 - a. identifikasi;
 - b. deteksi;
 - c. proteksi; dan
 - d. penanggulangan dan pemulihan.
- (2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.
- (3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.
- (4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.
- (5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 17

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 Pemerintah

Daerah wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.

- (2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.
- (3) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 18

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

Pasal 19

- (1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 14 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
- (2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

- (1) Perangkat Daerah melaksanakan audit Keamanan Informasi di lingkup pemerintah daerah.

- (2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
- (3) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 21

- (1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d dilaksanakan oleh Perangkat Daerah.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
 - a. kepala daerah dan wakil;
 - b. perangkat daerah;
 - c. pegawai atau aparatur sipil negara pada pemerintah daerah; dan
 - d. pihak lainnya.

Pasal 22

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

- a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
- b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
- c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
- d. perlindungan Informasi melalui penyediaan perangkat teknologi Keamanan Informasi dan jaring komunikasi sandi;
- e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;

- f. audit Keamanan Sistem Elektronik;
- g. audit keamanan pelaksanaan sistem manajemen;
- h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan pemerintah daerah dan Publik ;
- i. peningkatan kompetensi sumber daya manusia di bidang Keamanan Informasi dan/atau persandian;
- j. pengelolaan pusat operasi Pengamanan Informasi;
- k. penanganan insiden Keamanan Sistem Elektronik;
- l. forensik digital;
- m. perlindungan Informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
- n. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan pemerintah daerah melalui kegiatan kontra penginderaan;
- o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
- p. jenis Layanan Keamanan Informasi lainnya.

Pasal 23

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

- (4) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH PROVINSI DAN KABUPATEN/KOTA

Pasal 24

- (1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota sebagaimana dimaksud dalam Pasal 3 huruf b ditetapkan oleh Gubernur dan Bupati/Wali Kota.
- (2) Penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota sebagaimana dimaksud pada ayat (1) untuk menentukan jaring komunikasi sandi internal pemerintah daerah.
- (3) Jaring komunikasi sandi internal pemerintah daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
 - a. jaring komunikasi sandi antar perangkat daerah;
 - b. jaring komunikasi sandi internal perangkat daerah;
 - dan
 - c. jaring komunikasi sandi pimpinan daerah.
- (4) Jaring komunikasi sandi antar perangkat daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh perangkat daerah.
- (5) Jaring komunikasi sandi internal perangkat daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal perangkat daerah.
- (6) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Gubernur atau Bupati/Wali Kota, wakil Gubernur atau Bupati/Wali Kota, dan kepala perangkat daerah.

Pasal 25

- (1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota sebagaimana dimaksud dalam Pasal 24 ayat (1) dilaksanakan melalui:
 - a. identifikasi pola hubungan komunikasi sandi; dan
 - b. analisis pola hubungan komunikasi sandi.
- (2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
 - a. pola hubungan komunikasi pimpinan dan pejabat struktural internal pemerintah daerah;
 - b. alur informasi yang dikomunikasikan antar perangkat daerah dan internal perangkat daerah;
 - c. teknologi informasi dan komunikasi;
 - d. infrastruktur komunikasi; dan
 - e. kompetensi personel.
- (3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3).
- (4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) memuat:
 - a. pengguna Layanan yang akan terhubung dalam jaring komunikasi sandi;
 - b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan;
 - c. perangkat keamanan teknologi Informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
- (5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (5) ditetapkan sebagai pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota oleh Gubernur atau Bupati/Wali Kota dalam bentuk keputusan.

- (6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
 - a. entitas Pengguna Layanan yang terhubung dalam jaringan komunikasi sandi;
 - b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
 - c. sarana dan prasarana yang digunakan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
- (7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh:
 - a. Gubernur kepada Kepala BSSN; dan
 - b. Bupati/Wali Kota kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB IV

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 26

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah provinsi dan kabupaten/kota dan penetapan pola hubungan komunikasi sandi antar perangkat daerah.
- (2) Perangkat Daerah melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.
- (3) Perangkat Daerah kabupaten/kota menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati/Wali Kota dan Gubernur sebagai wakil Pemerintah Pusat.
- (4) Perangkat Daerah provinsi menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dan laporan hasil pemantauan dan evaluasi kabupaten/kota sebagaimana dimaksud pada ayat (3) kepada Gubernur dan Kepala BSSN.

Pasal 27

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah provinsi dan kabupaten/kota dan penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 28

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah provinsi dan kabuten/kota dan penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota dilaksanakan oleh BSSN dan Gubernur sebagai wakil Pemerintah Pusat sesuai dengan kewenangannya.

Pasal 29

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah provinsi dan kabuten/kota dan penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 30

- (1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 28 BSSN dan pemerintah daerah provinsi sesuai dengan kewenangannya menyelenggarakan rapat koordinasi urusan Persandian.
- (2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam setahun.

BAB VI
PENDANAAN

Pasal 31

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah provinsi dan kabupaten/kota dan penetapan pola hubungan komunikasi sandi antar perangkat daerah provinsi dan kabupaten/kota bersumber dari:

- a. Anggaran Pendapatan dan Belanja Daerah provinsi;
- b. Anggaran Pendapatan dan Belanja Daerah kabupaten/kota; dan/atau
- c. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII
KETENTUAN PENUTUP

Pasal 32

Pada saat Peraturan Badan ini mulai berlaku, 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) dicabut dan dinyatakan tidak berlaku.

Pasal 33

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Badan ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 20 Agustus 2019

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 16 September 2019

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

WIDODO EKATJAHJANA