SALINAN

GUBERNUR JAWA BARAT

PERATURAN GUBERNUR JAWA BARAT

NOMOR 41 TAHUN 2022

TENTANG

PERATURAN PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH PROVINSI JAWA BARAT

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR JAWA BARAT,

Menimbang : bahwa menindaklanjuti ketentuan Pasal 50 Peraturan Daerah Provinsi Jawa Barat Nomor 4 Tahun 2021 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik, dan Persandian, perlu menetapkan Peraturan Gubernur tentang Peraturan Pelaksanaan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi Jawa Barat;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 1950 tentang Pembentukan Propinsi Jawa Barat (Berita Negara Republik Indonesia tanggal 4 Juli 1950) jo. Undang-Undang Nomor 20 Tahun 1950 tentang Pemerintahan Jakarta Raya (Lembaran Negara Republik Indonesia Tahun 1950 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 15) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 29 Tahun 2007 tentang Pemerintahan Provinsi Daerah Khusus Ibukota Jakarta sebagai Ibukota Negara Kesatuan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 93, Tambahan Lembaran Negara Republik Indonesia Nomor 4744) dan Undang-Undang Nomor 23 Tahun 2000 tentang Pembentukan Provinsi Banten (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 4010);

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) 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 Nomor 5952);

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 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Kepala 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);
8. Peraturan Daerah Provinsi Jawa Barat Nomor 4 Tahun 2021 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik dan Persandian (Lembaran Daerah Provinsi Jawa Barat Tahun 2021 Nomor 4, Tambahan Lembaran Daerah Provinsi Jawa Barat Nomor 248);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG PERATURAN PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH PROVINSI JAWA BARAT.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini, yang dimaksud dengan:

1. Daerah Provinsi adalah Daerah Provinsi Jawa Barat.
2. Pemerintah Daerah Provinsi adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah Provinsi.
3. Gubernur adalah Gubernur Jawa Barat.
4. Pemerintah Daerah Kabupaten/Kota adalah Pemerintah Daerah Kabupaten/Kota di Daerah Provinsi.

5. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah Provinsi dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah Provinsi.
6. Dinas adalah Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
7. Badan Siber dan Sandi Negara yang selanjutnya disebut BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
8. 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.
9. Persandian adalah kegiatan di bidang pengamanan sistem Informasi yang dilaksanakan dengan menerapkan konsep, teori dan seni dari ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terikat pada etika profesi sandi.
10. Jaring Komunikasi Sandi adalah keterhubungan antar Pengguna Persandian melalui jaring telekomunikasi yang memanfaatkan persandian dalam komunikasi.
11. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan.
12. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
13. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
14. Pola Hubungan Komunikasi Sandi yang selanjutnya disingkat PHKS adalah bentuk atau pola hubungan antara dua entitas atau lebih dalam proses pengiriman dan penerimaan Informasi/pesan/berita secara aman menggunakan Persandian.
15. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik.
16. 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.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman bagi Dinas dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah Provinsi.

(2) Tujuan pelaksanaan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah Provinsi, yaitu:

a. menciptakan harmonisasi dalam melaksanakan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah Provinsi;

b. meningkatkan komitmen, efektivitas dan kinerja Dinas dalam melaksanakan kebijakan, program dan kegiatan pelaksanaan Persandian untuk Pengamanan Informasi; dan

c. memberikan pedoman bagi Dinas dalam menetapkan PHKS antar Perangkat Daerah.

Pasal 3

Ruang lingkup Peraturan Gubernur ini meliputi:

a. penyelenggaraan Persandian untuk Pengamanan Informasi; dan

b. penetapan PHKS antar Perangkat Daerah.

BAB II

PENYELENGGARAAN PERSANDIAN

UNTUK PENGAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 4

(1) Penyelenggaraan Persandian 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) Dinas bertanggungjawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1).

(3) Dinas melakukan pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi di Kabupaten/Kota melalui perangkat daerah/unit kerja yang melaksanakan urusan pemerintahan bidang persandian.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Paragraf 1

Umum

Pasal 5

(1) 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/atau

c. menetapkan aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi.

(2) Hasil dari penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud pada Pasal 4 ayat (1) menjadi pedoman bagi setiap Perangkat Daerah dalam melaksanakan Pengamanan Informasi di lingkungannya.

Paragraf 2

Rencana Strategis Pengamanan Informasi

Pasal 6

(1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a disusun oleh Dinas.

(2) Rencana strategis Pengamanan Informasi 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 (RPJPD), Rencana Pembangunan Jangka Menengah Daerah (RPJMD), Rencana Kerja Pembangunan Daerah (RKPD), Rencana Strategis Dinas, dan Rencana Kerja Dinas berdasarkan ketentuan peraturan perundang-undangan.

Pasal 7

(1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (1) yang merupakan bagian dari Renstra Dinas memuat:

a. tujuan;

b. sasaran;

c. program; dan

d. kegiatan.

(2) Dalam menjabarkan rencana strategis Pengamanan Informasi, Dinas menyusun rencana kerja Pengamanan Informasi yang merupakan bagian dari Rencana Kerja Dinas.

(3) Rencana kerja Pengamanan Informasi sebagaimana dimaksud pada ayat (2) memuat:

a. program;

b. kegiatan;

c. lokasi;

d. kelompok sasaran;

e. indikator kinerja program dan kegiatan; dan

f. anggaran.

Paragraf 3

Arsitektur Keamanan Informasi

Pasal 8

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b disusun oleh Dinas dan ditetapkan Kepala Dinas.

(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) Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

(5) Arsitektur Keamanan Informasi yang telah ditetapkan dilakukan evaluasi oleh Dinas pada tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

(6) Ketentuan lainnya terkait Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) dapat digantikan dengan Arsitektur Keamanan SPBE yang menjadi satu kesatuan dalam Arsitektur SPBE Nasional.

Paragraf 4

Tata Kelola Keamanan Informasi

Pasal 9

(1) Aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c disusun oleh Dinas dan ditetapkan Kepala Dinas.

(2) Aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi:

a. keamanan sumber daya teknologi Informasi;

b. keamanan akses kontrol;

c. keamanan data dan Informasi;

d. keamanan aplikasi SPBE;

e. keamanan jaringan;

f. keamanan surat elektronik;

g. keamanan pusat data;

h. keamanan komunikasi; dan/atau

i. keamanan lain sesuai kebutuhan.

(3) Dalam kondisi tertentu, masing-masing Perangkat Daerah dapat menyusun dan menetapkan aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi di lingkungannya setelah terlebih dahulu berkoordinasi dan berkonsultasi dengan Dinas.

(4) Dalam melakukan penyusunan aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1), Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Paragraf 1

Umum

Pasal 10

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b dilaksanakan oleh Dinas.

(2) Pengelolaan sumber daya keamanan Informasi sebagaimana dimaksud dalam ayat (1), terdiri atas:

a. pengelolaan aset keamanan teknologi Informasi dan komunikasi;

b. pengelolaan sumber daya manusia; dan

c. manajemen pengetahuan.

(3) Dalam melaksanakan pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) Dinas dapat berkoordinasi dengan Perangkat Daerah.

(4) Dalam hal tertentu, Perangkat Daerah dapat mengelola sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) setelah berkoordinasi, berkonsultasi dan mendapat rekomendasi dari Dinas.

Paragraf 2

Pengelolaan Aset Keamanan Teknologi Informasi

dan Komunikasi

Pasal 11

(1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai 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.

Paragraf 3

Pengelolaan Sumber Daya Manusia

Pasal 12

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b dilakukan oleh Dinas.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses, sebagai berikut:

a. perencanaan;

b. pengembangan kompetensi;

c. pembinaan karir;

d. pendayagunaan; dan

e. pemberian tunjangan pengamanan persandian.

Pasal 13

(1) Perencanaan sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf a dilaksanakan dengan ketentuan:

a. menyusun kebutuhan sumber daya manusia sesuai dengan hasil analisis beban kerja dan formasi jabatan; dan

b. menyusun standar kompetensi sesuai ketentuan peraturan perundang-undangan.

(2) Hasil perencanaan sebagaimana dimaksud pada ayat (1) disampaikan kepada Perangkat Daerah yang melaksanakan fungsi penunjang kepegawaian untuk dapat dipenuhi.

(3) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf b dilaksanakan dengan ketentuan:

a. melalui tugas belajar, pendidikan dan pelatihan, pembentukan dan penjenjangan fungsional, 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, instansi lainnya, atau Pemerintah Daerah Provinsi/Pemerintah Daerah Kabupaten/Kota masing-masing; dan

c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.

(4) Pembinaan karir sebagaimana dimaksud pada Pasal 12 ayat (2) huruf c dilaksanakan dengan ketentuan:

a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan

b. pengisian formasi jabatan pimpinan tinggi, jabatan *administrator*, jabatan pengawas, atau jabatan fungsional sesuai dengan standar kompetensi yang ditetapkan.

(5) Pendayagunaan sebagaimana dimaksud pada Pasal 12 ayat (2) huruf d dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi pegawai yang telah ditetapkan serta tidak dilakukan mutasi kecuali dalam rangka promosi.

(6) Pemberian tunjangan pengamanan persandian sebagaimana dimaksud pada Pasal 12 ayat (2) huruf e dilaksanakan melalui pemberian tunjangan khusus kepada sumber daya manusia yang bekerja melaksanakan urusan pemerintahan bidang Persandian sesuai ketentuan peraturan perundang-undangan dan kemampuan daerah.

Paragraf 4

Manajemen Pengetahuan

Pasal 14

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilaksanakan oleh Dinas.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dapat berupa terciptanya kegiatan atau sistem berbagi pengetahuan atau perkembangan terkait keamanan informasi dari hasil kegiatan pengembangan kompetensi sebagaimana dimaksud pada Pasal 13 ayat (1) huruf a dan b.

(3) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.

(4) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi di Pemerintah Daerah Provinsi.

(5) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah Provinsi berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

(6) Ketentuan lebih lanjut mengenai pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah Provinsi disusun oleh Dinas dan ditetapkan Kepala Dinas.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 15

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

Pasal 16

(1) Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 terdiri atas:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan 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 17

(1) Dalam melaksanakan pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16, Dinas 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 SPBE berfungsi kembali dengan baik.

Pasal 18

(1) Dalam melaksanakan pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16, Perangkat Daerah 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) Penerbitan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 19

(1) Dalam mendukung penyelenggaraan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 18 ayat (1) Dinas 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 20

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 15 dilakukan pada tahapan pemprosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.

(2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 21

(1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah Provinsi.

(2) Audit keamanan Informasi meliputi audit keamanan Sistem Elektronik, Audit keamanan SPBE dan/atau audit pelaksanaan sistem manajemen Keamanan Informasi.

(3) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 22

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d dilaksanakan oleh Dinas.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:

a. Gubernur dan Wakil Gubernur;
b. Sekretaris Daerah
c. Asisten Sekretaris Daerah
d. Kepala Perangkat Daerah/kepala unit kerja;
e. Aparatur Sipil Negara atau pegawai pada Pemerintah Daerah Provinsi; dan
f. pihak lainnya sesuai kebutuhan.

Pasal 23

(1) Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 22 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 atau audit keamanan SPBE;
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 Informasi;

l. forensik digital;

m. perlindungan Informasi pada kegiatan Pemerintah Daerah Provinsi melalui teknik pengamanan gelombang frekuensi atau sinyal.

n. perlindungan informasi pada aset/fasilitas penting milik atau yang akan digunakan oleh Pemerintah Daerah Provinsi melalui kegiatan kontra penginderaan;

o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau

p. jenis Layanan Keamanan Informasi lainnya.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan memperhatikan ketersediaan sumber daya.

(3) Ketentuan lebih lanjut mengenai Layanan Keamanan Informasi akan diatur dalam Pedoman Layanan Keamanan Informasi yang disusun oleh Dinas dan ditetapkan Kepala Dinas.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH PROVINSI

Pasal 24

(1) Penetapan PHKS antar perangkat daerah provinsi sebagaimana dimaksud dalam Pasal 3 huruf b disusun oleh Dinas dan ditetapkan oleh Gubernur.

(2) Penetapan PHKS antar Perangkat Daerah Provinsi sebagaimana dimaksud pada ayat (1) untuk menentukan Jaring Komunikasi Sandi Internal Pemerintah Daerah Provinsi.

Pasal 25

(1) Penyelenggaraan Jaring Komunikasi Sandi internal Pemerintah Daerah Provinsi sebagaimana dimaksud dalam Pasal 24 ayat (2) merupakan implementasi PHKS yang dilakukan di lingkungan Pemerintah Daerah Provinsi untuk mengamankan Informasi, sehingga komunikasi dan koordinasi dapat dilaksanakan secara aman, utuh, dan tidak bisa disangkal.

(2) Dinas mengelola dan memfasilitasi penyelenggaraan Jaring Komunikasi Sandi Internal Pemerintah Daerah Provinsi untuk Pengamanan Informasi yang dikecualikan di Pemerintah Daerah Provinsi.

(3) Jaring Komunikasi Sandi Internal Pemerintah Daerah Provinsi sebagaimana dimaksud pada ayat (1) 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 PD 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, Wakil Gubernur, dan Kepala Perangkat Daerah.

Pasal 26

(1) Untuk kelancaran pelaksanaan PHKS, Dinas dapat melakukan kerja sama dengan kementerian/lembaga yang menyelenggarakan tugas pemerintahan di bidang Persandian dan Keamanan Informasi serta antar Pemerintah Daerah dan Pemerintah Daerah Kabupaten/Kota.

(2) Pemerintah Daerah Provinsi dapat melakukan kegiatan operasional Jaring Komunikasi Sandi secara mandiri berkoordinasi dengan BSSN.

(3) Tata cara kerja sama sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Pasal 27

Penetapan PHKS antar perangkat daerah provinsi sebagaimana dimaksud dalam Pasal 24 ayat (1) dilakukan melalui:

a. identifikasi pola hubungan komunikasi sandi; dan

b. analisis pola hubungan komunikasi sandi.

Pasal 28

Identifikasi PHKS sebagaimana dimaksud dalam Pasal 27 huruf a, dilakukan terhadap:

a. pola hubungan komunikasi pimpinan dan pejabat struktural di lingkungan Pemerintah Daerah Provinsi;

b. alur Informasi yang dikomunikasikan antar Perangkat Daerah dan internal perangkat daerah;

c. teknologi Informasi dan komunikasi yang digunakan oleh pimpinan dan pejabat di Pemerintah Daerah Provinsi;

d. infrastruktur komunikasi yang ada di wilayah Pemerintah Daerah Provinsi; dan

e. kompetensi personil yang dibutuhkan.

Pasal 29

(1) Analisis PHKS sebagaimana dimaksud dalam Pasal 27 huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi.

(2) Analisis PHKS sebagaimana dimaksud pada ayat (1) 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.

(3) Hasil analisis PHKS sebagaimana dimaksud pada ayat (2) ditetapkan sebagai PHKS antar Perangkat Daerah Provinsi oleh Gubernur dalam bentuk keputusan.

(4) Keputusan sebagaimana dimaksud pada ayat (3) paling sedikit memuat:

a. entitas Pengguna Layanan yang terhubung dalam jaring 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

BAB IV

PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 30

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi dan penetapan PHKS.

(2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) minimal setiap 1 (satu) tahun sekali.

(3) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (2) huruf a dilaksanakan melalui kegiatan:

a. monitoring terhadap pemanfaatan aset teknologi komunikasi dan informasi; atau

b. monitoring terhadap pelaksanaan kebijakan manajemen risiko dan penerapan keamanan informasi oleh perangkat daerah.

(4) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan melalui kegiatan:

a. pengukuran tingkat pemanfaatan dan kepuasan layanan keamanan informasi oleh Perangkat Daerah;

b. penilaian mandiri atau evaluasi terhadap penyelenggaraan Persandian di Pemerintah Daerah Provinsi menggunakan instrumen evaluasi yang ditetapkan oleh BSSN;

c. pengukuran pencapaian kerja Dinas;

d. pemantauan dan evaluasi lainnya sesuai dengan ketentuan perundang-undangan.

(5) Kepala Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana pada ayat (2) huruf a kepada Gubernur.

(6) Kepala Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana pada ayat (2) huruf b dan laporan hasil pemantauan dan evaluasi di Kabupaten/Kota kepada Gubernur dan Kepala BSSN.

BAB V

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 31

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi dan penetapan PHKS antar Perangkat Daerah dilaksanakan oleh Dinas.

Pasal 32

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah kabupaten/kota dan penetapan PHKS antar perangkat daerah kabupaten/kota dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 33

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 31, Dinas menyelenggarakan rapat koordinasi urusan Persandian.

(2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling kurang 1 (satu) kali dalam setahun.

BAB VI

PENDANAAN

Pasal 34

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah Provinsi dan penetapan PHKS antar Perangkat Daerah bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah Provinsi; dan/atau

b. sumber lain yang sah sesuai ketentuan peraturan perundang-undangan.

BAB VII

KETENTUAN PENUTUP

Pasal 35

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Bandung
pada tanggal 5 Agustus 2022

GUBERNUR JAWA BARAT,

ttd

MOCHAMAD RIDWAN KAMIL

Diundangkan di Bandung
pada tanggal 5 Agustus 2022

SEKRETARIS DAERAH PROVINSI
JAWA BARAT,

ttd

SETIAWAN WANGSAATMAJA

BERITA DAERAH PROVINSI JAWA BARAT TAHUN 2022 NOMOR 42