SALINAN

BUPATI BANDUNG
PROVINSI JAWA BARAT
PERATURAN BUPATI BANDUNG

NOMOR 92 TAHUN 2021

TENTANG

PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BANDUNG,

Menimbang : a. bahwa sistem pemerintahan berbasis elektronik dilaksanakan berdasarkan prinsip keamanan yang meliputi kerahasiaan, keutuhan, ketersediaan, keaslian dan kenirsangkalan sumber daya yang mendukung sistem pemerintahan berbasis elektronik;

b. bahwa dalam menjamin terjaganya keamanan informasi sistem pemerintahan berbasis elektronik perlu dilaksanakan persandian untuk pengamanan informasi;

c. bahwa untuk mendukung keamanan sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Bandung serta terselanggaranya pelaksanaan persandian untuk mendukung pengamanan informasi diperlukan adanya pedoman manajemen keamanan dan pelaksanaan persandian;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Pelaksanaan Persandian untuk Pengamanan Informasi;

Mengingat : 1. Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah Kabupaten Dalam Lingkungan Jawa Barat (Berita Negara Republik Indonesia Tahun 1950) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1968 tentang Pembentukan Kabupaten Purwakarta dan Kabupaten Subang dengan mengubah Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah Kabupaten Dalam Lingkungan Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Tahun 1950 Nomor 2851);

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 Republik Indonesia Nomor 5952);

3. 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);

4. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);

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 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 1051);
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
9. Peraturan Bupati Nomor 69 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Bandung Tahun 2021 Nomor 69);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Bandung.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Bandung.
4. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
5. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan Pemerintahan Daerah di bidang Komunikasi dan Informatika.

6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
7. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
8. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan Keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
9. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
10. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
11. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
12. 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.
13. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi Informasi dan komunikasi secara elektronik ataupun non elektronik.
14. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
15. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
16. 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 ini serta Informasi lain yang berkaitan dengan kepentingan publik.

17. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
18. 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.
19. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
20. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
21. Badan Siber dan Sandi Negara yang selanjutnya ~~disebut~~ disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

BAB II
PENYELENGGARAAN MANAJEMEN KEAMANAN INFORMSI SPBE

Bagian Kesatu
Umum

Pasal 2

(1) Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE dan Aplikasi SPBE.
(2) Penjaminan kerahasiaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan lainnya.
(3) Penjaminan keutuhan sebagaimana dimaksud pada ayat (1) dilakukan melalui pendeteksian modifikasi.
(4) Penjaminan ketersediaan sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan cadangan dan pemulihan.

(5) Penjaminan keaslian sebagaimana dimaksud pada ayat (1) dilakukan melalui penyediaan mekanisme verifikasi dan validasi.
(6) Penjaminan kenirsangkalan (*nonrepudiation*) sebagaimana dimaksud pada ayat (1) dilakukan melalui penerapan tanda tangan elektronik dan jaminan pihak ketiga terpercaya melalui penggunaan Sertifikat Elektronik.

Pasal 3

Area yang menjadi prioritas dalam penyelenggaraan Manajemen Keamanan SPBE di Pemerintah Daerah meliputi:
a. Data dan Informasi SPBE;
b. Aplikasi SPBE;
c. Aset Infrastruktur SPBE; dan
d. Kebijakan keamanan informasi SPBE;

Bagian Kedua
Penanggung Jawab
Pasal 4

(1) Penanggung jawab Manajemen Keamanan SPBE dijabat oleh Sekretaris Daerah.
(2) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, Sekretaris Daerah disebut sebagai koordinator SPBE.
(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, koordinator SPBE sebagaimana dimaksud pada ayat (2) menetapkan pelaksana teknis Keamanan SPBE.
(4) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (3) dilaksanakan oleh Dinas.

Pasal 5

Dinas sebagaimana dimaksud dalam Pasal 4 ayat (4) mempunyai tugas:
a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
c. melaporkan pelaksanaan Manajemen Keamanan SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE Pemerintah Daerah;
d. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis

dan prosedur Keamanan SPBE yang telah ditetapkan; dan

e. memastikan keberlangsungan proses bisnis SPBE;

Bagian Ketiga

Perencanaan

Pasal 6

(1) Perencanaan dilakukan oleh pelaksana teknis Keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
   a. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan
   b. target realisasi program kerja Keamanan SPBE.

(3) Dinas menyusun program kerja keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE.

(4) Program kerja Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) disusun berdasarkan kategori risiko Keamanan SPBE sesuai dengan peraturan perundang-undangan.

Pasal 7

(1) Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:
   a. sosialisasi; dan
   b. pelatihan.

(2) Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf b dilaksanakan paling sedikit melalui:
   a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
   b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
   c. mengukur tingkat risiko Keamanan SPBE

(3) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE sebagaimana dimaksud pada (2).

(4) Peningkatan Keamanan SPBE dilaksanakan paling sedikit melalui:
   a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
   b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

(5) Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf d dilaksanakan paling sedikit melalui:
   a. mengidentifikasi sumber serangan;
   b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
   c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
   d. mendokumentasi bukti insiden yang terjadi; dan
   e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.

(6) Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keempat
Dukungan Pengoperasian
Pasal 8

(1) Dukungan pengoperasian dilakukan oleh koordinator SPBE.

(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
   a. sumber daya manusia Keamanan SPBE; dan
   b. anggaran Keamanan SPBE.

(3) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit harus memiliki kompetensi:
   a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan
   b. keamanan aplikasi.

(4) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (3), Pemerintah Daerah paling sedikit melakukan kegiatan:
   a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan
   b. bimbingan teknis mengenai standar Keamanan SPBE.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Evaluasi Kinerja
Pasal 9

(1) Evaluasi kinerja dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Keamanan SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
    b. menetapkan indikator kinerja pada setiap area proses;
    c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
    d. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan
    e. mendukung dan merealisasikan program audit Keamanan SPBE
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Keenam
Perbaikan Berkelanjutan
Pasal 10

(1) Perbaikan berkelanjutan dilakukan oleh Dinas.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
    a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
    b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB III

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 11

Penyelenggaraan Persandian pada Pemerintah Daerah meliputi:

a. penyelenggaraan Persandian untuk Pengamanan Informasi SPBE Pemerintah Daerah; dan
b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 12

(1) Penyelenggaraan Persandian pada Pemerintah Daerah sebagaimana dimaksud dalam Pasal 11 huruf a dilaksanakan melalui:
    a. penyusunan kebijakan Pengamanan Informasi;
    b. pengelolaan sumber daya Keamanan Informasi;
    c. pengamanan Sistem Elektronik dan Pengamanan Informasi non elektronik; dan
    d. penyediaan Layanan Keamanan Informasi.
(2) Dinas bertanggung jawab terhadap Penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) untuk Pengamanan Informasi.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 13

(1) Pemerintah Daerah menyusun kebijakan Pengamanan Informasi mengacu pada norma, standar, prosedur, dan kriteria yang ditetapkan oleh lembaga pemerintahan di bidang keamanan siber.
(2) Kebijakan Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan dengan:
    a. menyusun rencana strategis pengamanan Informasi;
    b. menetapkan Arsitektur Keamanan Informasi; dan
    c. menetapkan aturan mengenai tata Kelola Keamanan Informasi.

Pasal 14

(1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf a disusun oleh Bupati.

(2) Dalam Menyusun rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) Bupati menugaskan kepada Dinas.
(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 diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
(5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada Kepala Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.
(6) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (5) Bupati menunjuk Dinas.

Pasal 15

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b ditetapkan oleh Bupati.
(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) Bupati dapat melakukan koordinasi dan konsultasi kepada Kepala Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.
(4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Bupati menunjuk Dinas.
(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 Bupati pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 16

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf c ditetapkan oleh Bupati.
(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) Bupati dapat melakukan koordinasi dan konsultasi kepada Kepala Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.
(4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Bupati menunjuk Dinas.

Bagian Ketiga
Pengelolaan Sumber Daya Keamanan Informasi
Pasal 17

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 12 ayat (1) huruf b dilaksanakan oleh Dinas.
(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 18

(1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 17

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 19

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf b dilakukan oleh Perangkat Daerah yang membidangi kepegawaian dan pengembangan sumber daya manusia.

(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 20

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf a dilaksanakan dengan ketentuan:
   a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan 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 19 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 19 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 21

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf c dilakukan oleh Dinas.
(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 Kepala Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Bagian Keempat
Pengamanan Sistem Elektronik dan Pengamanan Informasi Non elektronik

Pasal 22

Pengamanan Sistem Elektronik dan pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 12 ayat (1) huruf c dilaksanakan oleh Dinas.

Pasal 23

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 22 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 24

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 23 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 pelindungan 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 25

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 23 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 26

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 25 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 27

(1) Pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 22 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi non elektronik.
(2) Pengamanan Informasi non elektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 28

(1) Dinas 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 29

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 12 ayat (1) huruf d dilaksanakan oleh Dinas.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
   a. Bupati dan wakil Bupati;
   b. Perangkat Daerah;
   c. pegawai pada Pemerintah Daerah; dan
   d. pihak lainnya.

Pasal 30

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 31

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 30 Dinas 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.

BAB IV

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 32

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 11 huruf b ditetapkan oleh Bupati.
(2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah 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 Bupati, wakil Bupati dan kepala Perangkat Daerah.

Pasal 33

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 32 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 (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).

(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) 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 dalam bentuk keputusan.

(6) Keputusan sebagaimana dimaksud pada ayat (5) 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.

(7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Bupati kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB V
PEMANTAUAN, EVALUASI, DAN PELAPORAN
Pasal 34

(1) Dinas melakukan pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Manajemen Keamanan SPBE dan Persandian untuk Pengamanan Informasi dan penetepan pola hubungan komunikasi sandi antar Perangkat Daerah.
(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) paling sedikit dilaksanakan 1 (satu) tahun sekali.
(3) Laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) disampaikan kepada BSSN secara berjenjang melalui Bupati dan gubernur.

Pasal 35

Pemantauan, evaluasi, dan pelaporan terhadap Manajemen Keamanan SPBE dan Persandian untuk Pengamanan Informasi dan penetepan pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII
PENDANAAN
Pasal 36

Pendanaan pelaksanaan penyelenggaraan Manajemen Keamanan SPBE dan Persandian untuk Pengamanan Informasi dan penetepan pola hubungan komunikasi sandi antar Perangkat Daerah bersumber dari:
a. APBD
b. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB IX
KETENTUANPENUTUP
Pasal 37

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang dapat mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Bandung.

Ditetapkan di Soreang
pada tanggal 8 November 2021

BUPATI BANDUNG,

ttd

M. DADANG SUPRIATNA

Diundangkan di Soreang
pada tanggal 8 November 2021

SEKRETARIS DAERAH
KABUPATEN BANDUNG,

ttd

CAKRA AMIYANA

BERITA DAERAH KABUPATEN BANDUNG TAHUN 2021 NOMOR 92

Salinan sesuai dengan aslinya
Plt KEPALA BAGIAN HUKUM

DICKY ANUGRAH, SH, M.Si
Pembina Tk. I
NIP. 19740717 199803 1 003