SALINAN

BUPATI BANDUNG
PROVINSI JAWA BARAT

PERATURAN BUPATI BANDUNG

NOMOR 131 TAHUN 2018

TENTANG

KEAMANAN INFORMASI DI LINGKUNGAN
PEMERINTAH KABUPATEN BANDUNG

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BANDUNG,

Menimbang : a. bahwa penerapan keamanan informasi akan memastikan terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan informasi setiap waktu dapat berjalan dengan baik di lingkungan pemerintahan Kabupaten Bandung;

b. bahwa untuk mendukung penyelenggaraan keamanan informasi yang terkelola dengan baik agar dapat menjaga seluruh sumber daya informasi secara efisien dan efektif serta terciptanya sinergi di antara Perangkat Daerah di lingkungan pemerintah kabupaten Bandung, perlu ditetapkan peraturan Bupati tentang Penerapan keamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b perlu menetapkan Peraturan Bupati tentang Keamanan Informasi di lingkungan Pemerintah Kabupaten Bandung

Mengingat : 1. Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Propinsi Jawa Barat (Berita Negara 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-Daerah Kabupaten Dalam Lingkungan Propinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);

2. 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 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);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2008 Nomor 58 Tambahan Lembaran Negara Nomor 4843);

4. Peraturan Presiden Nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;

5. Keputusan Presiden Nomor 20 tahun 2006 tentang Dewan Teknologi Informasi dan Komunikasi Nasional;

6. Peraturan Menteri Komunikasi dan Informatika Nomor: 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;

7. Keputusan Menteri Komunikasi dan Informasi Nomor: 57/KEP/M.KOMINFO/12/2003 tentang Panduan Penyusunan Rencana Induk Pengembangan E-Government Lembaga;

8. Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi;

9. Peraturan Kepala Lembaga Sandi Negara Nomor 17 Tahun 2017 Pedoman Penyelenggaraan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintahan Daerah Provinsi dan Kabupaten/Kota;

10. Peraturan Daerah Kabupaten Bandung Nomor 12 Tahun 2013 tentang Partisipasi dan Keterbukaan Informasi Publik dalam Penyelenggaraan Pemerintahan di Kabupaten Bandung (Lembaran Daerah Kabupaten Bandung Tahun 2013 Nomor 12);

11. Peraturan Daerah Kabupaten Bandung Nomor 12 Tahun 2016 Tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Bandung Tahun 2016 Nomor 12);

12. Peraturan Bupati Bandung Nomor 16 Tahun 2016 tentang Kebijakan Umum Penyelanggaraan e-Government di Lingkungan Pemerintah Kabupaten Bandung (Berita Daerah Kabupaten Bandung Tahun 2016 Nomor 16);

13. Peraturan Bupati Bandung Nomor 17 Tahun 2016 tentang Tata Kelola Infrastruktur Teknologi dan Komunikasi di Lingkungan Pemerintah Kabupaten Bandung (Berita Daerah Kabupaten Bandung Tahun 2016 Nomor 17);

14. Peraturan Bupati Bandung Nomor 18 Tahun 2016 tentang Tata kelola Kelembagaan dan Sumber Daya Manusia Teknologi Informasi dan Komunikasi di Lingkungan Pemerintah Kabupaten Bandung (Berita Daerah Kabupaten Bandung Tahun 2016 Nomor 18);

15. Peraturan Bupati Bandung Nomor 19 Tahun 2016 tentang Tata kelola Aplikasi di Lingkungan Pemerintah Kabupaten Bandung (Berita Daerah Kabupaten Bandung Tahun 2016 Nomor 19);

16. Peraturan Bupati Nomor 105 tahun 2016 tentang Masterplan Teknologi Informasi dan Komunikasi dilingkungan pemerintahan Kabupaten Bandung (Berita Daerah Kabupaten Bandung Tahun 2016 Nomor 107);

17. Peraturan Bupati Nomor 71 tahun 2017 tentang Tata Kelola Data di lingkungan pemerintahan Kabupaten Bandung (Berita Daerah Kabupaten Bandung Tahun 2017 Nomor 71);

MEMUTUSKAN

Menetapkan : PERATURAN BUPATI TENTANG KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN BANDUNG

BAB I
KETENTUAN UMUM
Pasal 1

Dalam peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Bandung.

2. Pemerintah Daerah adalah Bupati dan perangkat daerah sebagai unsur penyelenggara pemerintahan daerah.

3. Bupati adalah Bupati Bandung.

4. Kecamatan dan desa adalah kecamatan dan desa di Kabupaten Bandung.
5. Perangkat Daerah yang selanjutnya disingkat PD adalah Perangkat Daerah di lingkungan Pemerintah Kabupaten Bandung.

6. Data adalah catatan atas kumpulan fakta atau deskripsi dari sesuatu/kejadian/kenyataan yang dihadapi berupa angka, karakter, simbol, gambar, peta, tanda, isyarat, tulisan, suara dan bunyi, yang merepresentasikan keadaan sebenarnya atau menunjukkan suatu ide, objek, kondisi, atau situasi.

7. 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.

8. Aset informasi adalah pengetahuan atau data yang memiliki nilai bagi organisasi/ Perangkat daerah.

9. *Intrussion Detection System* yang selanjutnya disingkat *IDS adalah* sebuah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan internet.

10. *Intrussion Prevention System* yang selanjutnya disingkat *IPS* adalah sebuah sistem yang menggabungkan fungsi firewall dan fungsi IDS dengan proporsional.

11. Kata sandi atau Password adalah kode atau simbol khusus untuk mengamankan sistem komputer yaitu untuk mengidentifikasi pihak yang mengakses data, program atau aplikasi komputer yang digunakan.

12. Event log adalah file yang terdapat pada komputer untuk mencatat informasi mengenai kegiatan user dan atau sistem seperti waktu *log-in* dan *log-out.*

13. Virus adalah program yang bersifat merusak dan aktif dengan bantuan orang (dieksekusi) dan tidak dapat mereplikasi sendiri penyebarannya karena dilakukan oleh orang seperti disalin (dicopy), biasanya melalui *attachment*, email, game, perangkat lunak bajakan dan lainnya.

14. Enkripsi adalah alat untuk mencapai keamanan data dengan menerjemahkannya menggunakan sebuah kunci atau kata sandi sehingga mencegah kata sandi atau kunci agar tidak dapat dengan mudah dibaca pada file konfigurasi.

15. Informasi elektronik ialah informasi yang berbentuk atau tersimpan dalam media digital.

16. Informasi non elektronik ialah informasi yang berbentuk dokumen fisik hasil pengumpulan digital yang telah dicetak ataupun hasil pengumpulan secara manual.

17. Aset yang berhubungan dengan teknologi informasi ialah aset pendukung dalam pengelolaan aset informasi seperti sarana penyimpanan, pengolahan informasi dan sarana lainnya yang disesuaikan dengan aturan yang berlaku.

18. Firewall adalah peralatan untuk menjaga keamanan jaringan dengan melakukan pengawasan dan penyeleksian atas lalu lintas data/informasi melalui jaringan serta melakukan pemisahan jaringan private dan jaringan publik.

19. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan Kenirsangkalan informasi.

20. Kerahasiaan adalah aspek keamanan informasi yang menjamin informasi tidak dapat diketahui oleh siapapun kecuali pihak yang memiliki otoritas.

21. Keaslian atau Keautentikan adalah aspek keamanan informasi yang menjamin keaslian informasi baik secara kesatuan sistem maupun informasi itu sendiri.

22. Integritas adalah aspek keamanan informasi yang menjamin informasi tidak dapat diubah oleh siapapun kecuali pihak yang memiliki otoritas.

23. ketersediaan adalah aspek keamanan informasi yang menjamin informasi masih original tidak mendapatkan pengubahan dari pihak-pihak yang tidak bertanggung jawab.

24. Kenirsangkalan adalah aspek keamanan informasi yang menjamin informasi tidak dapat disangkal oleh pihak pengirim maupun penerima.

25. Risiko keamanan informasi adalah potensi bahwa suatu ancaman akan mengeksploitasi kelemahan satu atau sekelompok aset dan karenanya membahayakan organisasi.

26. Manajemen proyek adalah semua bentuk kegiatan yang melibatkan pihak ketiga dan memerlukan akses informasi dari setiap Perangkat Daerah di Kabupaten Bandung seperti kajian, pembuatan masterplan, dokumen pengawasan proyek dan lainnya.

27. Perangkat Bergerak adalah perangkat telekomunikasi portable (HP), komputer portable (laptop, notebook), alat penyimpanaan portable (flashdisk, hard disk eksternal) dan alat serupa lainnya.

28. Teleworking adalah perangkat penyimpanan yang baerbasis situs teleworking (hosting, VPN dan lainnya).

29. Kriptografi adalah teknik enkripsi dimana “naskah asli” (*plaintext*) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (*ciphertext*) oleh seseorang yang tidak memiliki kunci dekripsi.

30. Pemasok adalah badan usaha, kelompok atau perseorangan dari pihak luar atau Pihak Ketiga selain unit organisasi pemerintahan Kabupaten Bandung yang terlibat dalam kegiatan/ proyek yang dilaksanakan oleh pemerintah Kabupaten Bandung

Pasal 2

Keamanan Informasi dilaksanakan sesuai azas penyelenggaraan *e-Government* dan aspek sebagai berikut:
a Kerahasiaan;
b Keaslian;
c Keutuhan;
d Ketersediaan; dan
e Kenirsangkalan;

BAB II

KEBIJAKAN KEAMANAN INFORMASI

Bagian Kesatu

Kebijakan Keamanan Informasi

Pasal 3

(1) Pemerintah Daerah bertanggung jawab dan berkomitmen terhadap Pengamanan Informasi.

(2) Informasi sebagaimana dimaksud pada ayat (1) dinyatakan sebagai salah satu aset penting Daerah.

(3) Perlindungan informasi Pemerintah Daerah dilaksanakan sesuai dengan tingkat sensitivitas, nilai dan kepentingannya.

(4) Informasi Pemerintah Daerah hanya digunakan untuk kepentingan internal birokasi dan layanan publik yang menjadi tanggung jawabnya.

(5) Semua akses, penggunaan dan pemrosesan informasi dilakukan sesuai dengan kebijakan, standar dan prosedur yang berlaku di lingkungan Pemerintah Daerah.

(6) Pelanggaran terhadap keamanan informasi merupakan pelanggaran hukum, sehingga akan diberlakukan sanksi sesuai ketentuan perundangan-undangan yang berlaku.

Bagian Kedua

Dokumen Penerapan Keamanan Informasi

Pasal 4

(1) Dokumen Penerapan keamanan informasi bertujuan untuk melindungi aset informasi pemerintah Daerah.

(2) Standar, Prosedur dan Pedoman yang mengatur hal terkait dengan keamanan informasi merupakan dokumen yang tidak terpisahkan dari Penerapan keamanan informasi.

(3) Dokumen Penerapan keamanan informasi dapat ditinjau ulang pada periode tertentu, sesuai dengan perkembangan dan kebutuhan perubahannya.

BAB III

ORGANISASI KEAMANAN INFORMASI

Bagian Kesatu

Peran dan Fungsi

Pasal 5

Pemerintah Daerah menetapkan peran dan fungsi pada setiap organisasi terhadap aset informasi sebagai berikut:
a. Pemilik informasi;
b. Pengelola informasi;
c. Pengguna informasi; dan
d. Petugas Keamanan Informasi.

Bagian Kedua

Tanggung Jawab ASN dan Perangkat Daerah

Pasal 6

(1) Setiap PD/Bidang/Seksi/Individu ASN bertanggung jawab atas keamanan informasi.

(2) Tanggung jawab atas keamanan informasi spesifik disertakan pada uraian tugas Bidang/Seksi/Individu ASN jika mempunyai akses ke informasi yang sensitif, berharga atau penting.

(3) Bentuk tanggung jawab Daerah/Bidang/Seksi/Individu ASN sebagaimana dimaksud pada ayat (1) ialah dengan menerapkan keamanan informasi kedalam manajemen proyek, perangkat bergerak dan teleworking.

BAB IV
PENGELOLAAN ASET INFORMASI
Bagian Kesatu
Jenis Aset
Pasal 7

Jenis aset informasi yang harus dilakukan pengamanan di lingkungan Pemerintahan Daerah adalah sebagai berikut:
a. Informasi elektronik;
b. Informasi non elektronik; dan
c. Aset yang berhubungan dengan teknologi informasi.

Bagian Kedua
Proses pengelolaan
Pasal 8

(1) Setiap PD harus melakukan inventarisasi, klasifikasi, evaluasi dan memutakhirkan aset informasi serta aset teknologi informasi sesuai dengan kewenangan dan peraturan yang berlaku.

(2) Aset informasi dan aset teknologi informasi harus ditempatkan pada lokasi atau tempat khusus yang aman.

(3) Setiap PD harus melakukan pengamanan informasi berupa penghapusan, penghancuran, pemindahan, penggandaan informasi yang tersimpan pada media yang akan dibuang.

(4) PD yang berwenang dan bertanggung jawab memimpin pengelolaan keamanan informasi di pemerintahan Kabupaten Bandung melakukan evaluasi dan penilaian keamanan informasi pada tiap Perangkat Daerah di pemerintahan Daerah sekurang-kurangnya setahun sekali.

(5) Penyelenggaraan evaluasi sebagaimana dimaksud pada ayat (4) harus berpedoman pada Sistem Manajemen Kemanan Informasi.

BAB V

KEAMANAN SUMBERDAYA MANUSIA

Pasal 9

(1) Dalam penerapan pengaman Informasi, pemilik informasi dapat menggunakan tenaga ahli internal ASN dan atau eksternal dengan sistem seleksi sesuai dengan aturan yang berlaku.

(2) Setiap PD harus melakukan pengecekan latar belakang tenaga Ahli jika mempunyai akses ke informasi yang sensitif, berharga atau penting di lingkungan pemerintah Daerah.

(3) PD yang berwenang dan bertanggung jawab memimpin pengelolaan keamanan informasi di lingkungan Pemerintahan Daerah secara berkala melakukan peningkatan pengetahuan pada sumber daya manusia keamanan informasi yang dapat dilaksanakan secara mandiri atau melibatkan PD lain yang mempunyai kewenangan dalam peningkatan kemampuan sumber daya manusia sesuai dengan aturan yang berlaku.

(4) Setiap PD yang mengunakan sumber daya manusia internal atau eksternal dalam penerapan keamanan dapat memberikan sanksi kepada sumber daya manusia yang melanggar aturan keamanan informasi sesuai dengan aturan yang berlaku.

BAB VI

KEAMANAN FISIK DAN LINGKUNGAN

Pasal 10

(1) Akses ke semua kantor, ruang komputer dan ruang kerja yang berisi informasi sensitif, berharga atau penting dibatasi secara fisik dan dilengkapi dengan peralatan keamanan yang sesuai.

(2) Akses ke area yang memiliki informasi sensitif, berharga atau penting hanya diperbolehkan kepada ASN yang berwenang atau personil yang telah mendapat izin.

(3) Akses oleh personil lainnya yang telah mendapatkan izin sebagaimana dimaksud pada ayat (2) diawasi oleh ASN yang berwenang.

(4) Pengguna harus *log off* dari komputer dan server saat telah selesai digunakan.

(5) Pengguna harus mematikan sesi aktif saat sudah selesai menggunakan layanan aplikasi, kecuali dapat dilindungi dengan mekanisme penguncian otomatis seperti *screen saver* yang dilengkapi kata sandi.

(6) Setiap ASN dan PD harus bertanggung jawab dan wajib melakukan koordinasi dengan unit pengelola TIK atas pembuangan informasi sensitif, berharga atau penting serta pembuangan peralatan kerja yang digunakan untuk menyimpan data dan informasi terkait secara aman.

BAB VII

MANAJEMEN KOMUNIKASI DAN OPERASI

Pasal 11

(1) Kegiatan operasi keamanan informasi dan layanan sistem informasi harus terdokumentasi.

(2) Administrator layanan sistem informasi dapat mengubah atau menghentikan hak akses dari ASN atau personil jika dicurigai atau diketahui mengganggu operasi layanan sistem atau menyimpang dari aturan yang telah ditetapkan.

(3) Setiap layanan aplikasi harus didukung oleh catatan (event log) yang memungkinkan semua aktivitas sistem dapat diketahui dalam waktu paling lambat 2 jam.

(4) Perubahan data dan informasi hanya dapat diubah oleh pihak yang berwenang sesuai dengan proses Penerapan data dan informasi yang telah ditetapkan.

(5) Aplikasi anti virus diinstall dan difungsikan pada semua *firewall*, *server*, *Personal Computer* dan *Laptop* milik Pemerintah Daerah.

(6) Data dan informasi yang bersifat sensitif, berharga atau penting dalam layanan sistem informasi wajib di-*backup* secara periodik.

(7) Data dan Informasi yang bersifat sensitif, berharga atau penting yang tersimpan dalam media backup disimpan secara terenkripsi diluar kantor pemerintahan daerah.

(8) Setiap PC dan Server dilingkungan pemerintah daerah harus dilengkapi dengan perangkat lunak anti virus yang secara otomatis melakukan scanning atas seluruh akses data dari dan ke mesin tersebut.

(9) Setiap pengguna PC dan server harus memastikan bahwa perangkat lunak anti virus yang terpasang selalu memiliki database virus yang terkini (*up to date*)

BAB VIII

PENGENDALIAN AKSES DAN KRIPTOGRAFI

Bagian Kesatu

Manajemen Akses

Pasal 12

(1) Setiap pengguna layanan aplikasi memiliki satu ID pengguna dan kata sandi yang unik, bersifat pribadi dan rahasia untuk digunakan mengakses ke komputer dan jaringan komputer di lingkungan pemerintah daerah.

(2) ID pengguna dapat dinonaktifkan atau diubah statusnya apabila terjadi perubahan status pengguna pada lingkungan pemerintah daerah.

(3) Akses data/informasi/layanan sistem informasi/wifi yang diberikan kepada pihak ketiga harus berdasarkan izin dari pengelola keamanan informasi pada tiap PD.

(4) Hak akses atas komputer dan layanan sistem informasi bagi pengguna dan administrator dibatasi berdasarkan tingkat kebutuhannya.

Bagian Kedua

Pengaturan Kata Sandi Pengguna

Pasal 13

(1) Kata sandi yang dikeluarkan oleh pengelola keamanan informasi memiliki masa pakai dalam jangka waktu tertentu.

(2) Kata sandi paling sedikit terdiri dari 8 (delapan) karakter dan sebaiknya menggunakan 3 kombinasi angka, huruf dan simbol.

(3) Kata sandi bukan merupakan:
a. sesuatu yang mudah ditebak atau mudah didapatkan oleh orang lain yang bersumber dari data pribadi; dan
b. urutan angka atau karakter yang sama atau berurut.

(4) Pengguna yang lupa atau tidak bisa menemukan kata sandinya harus melaporkan kepada pengelola keamanan informasi atau administrator layanan sistem informasi tersebut berada.

(5) Pengguna tidak boleh membuat kata sandi yang mudah ditebak dan tidak boleh ditulis atau diletakkan pada tempat yang dapat dilihat oleh pengguna lain.

Bagian Ketiga

Penggunaan dan Pengamanan Jaringan

Pasal 14

(1) Akses jaringan ke layanan sistem informasi secara rutin diperbaharui untuk mencegah pengguna mengakses situs-situs yang tidak berhubungan dengan kegiatan pemerintahan.

(2) Unit pengelola TIK kabupaten Bandung berhak memblokir, menyembunyikan, menolak, mengubah atau menghentikan layanan komunikasi data kapanpun jika dinilai terdapat ancaman pihak internal dan atau eksternal terhadap keamanan informasi.

(3) Akses terhadap semua port jaringan dikontrol dengan aman oleh unit pengelola TIK.

(4) Network port aktif yang tidak dijaga dan terhubung dengan jaringan komputer pemerintah kabupaten Bandung tidak boleh ditempatkan di area publik.

(5) Web server yang bisa diakses melalui internet diproteksi dengan router dan atau *firewall* yang disetujui oleh unit pengelola TIK kabupaten Bandung.

(6) Unit pengelola TIK kabupaten Bandung memonitor semua aktifitas layanan sistem informasi yang dijalankan guna menghindari terjadinya akses dan penggunaan sistem yang tidak bertanggung jawab.

(7) Pengujian secara berkala harus dilakukan terhadap keamanan jaringan komunikasi data.

(8) Teknologi *firewall*, *IDS* dan *IPS* harus digunakan untuk mengimplementasikan pengamanan akses yang memadai.

Bagian Ketiga

Kriptografi

Pasal 15

(1) Enkripsi dapat diimplementasikan untuk informasi yang sensitif, berharga atau penting di Daerah.

(2) Penggunaan, perlindungan dan masa dengan enkripsi enkripsi sebagaimana dimaksud pada ayat (1) pada prosesnya harus dikembangkan dan diimplentasikan oleh Unit/ Bidang yang bertanggung jawab pada urusan Persandian dengan memperhatikan aturan yang berlaku.

(3) Pada proses implementasi enkripsi Unit/ Bidang yang bertanggung jawab pada urusan Persandian dapat dibantu oleh tenaga ahli atau unit terkait pada level pemerintah provinsi atau pusat.

BAB IX

PENGEMBANGAN, AKUISISI & PEMELIHARAAN SISTEM INFORMASI

Pasal 16

Pengembangan, akuisisi dan pemeliharaan Sistem Informasi dilaksanakan berdasarkan Peraturan Bupati mengenai Tata Kelola Aplikasi dilingkungan Pemerintah Kabupaten Bandung dengan memperhatikan unsur keamanan informasi dan unsur-unsur risiko TI.

BAB X

MANAJEMEN HUBUNGAN PEMASOK

Pasal 17

Kebijakan yang harus dilaksanakan dalam upaya memastikan perlindungan keamanan informasi yang dapat diakses pemasok:

a Perangkat Daerah harus memasukan klausul perjanjian keamanan informasi jika bekerjasama pemasok dalam setiap pengadaan aset organisasi terutama yang berhubungan teknologi informasi dan komunikasi; dan
b Perjanjian kemanan informasi harus di reviu, audit dan dilakukan perubahan jika terdapat perubahan layanan pemasok sesuai dengan aturan yang berlaku.

BAB XI

MANAJEMEN INSIDEN

Bagian Kesatu

Mekanisme Layanan Keamanan Informasi Elektronik

Pasal 18

Tindakan yang harus dilaksanakan dalam menangani dan merespon insiden yang mengancam Keamanan Informasi elektronik:

a Pemilik Informasi mengidentifikasi permasalahan dan sumber kebocoran informasi elektronik;
b Pemilik Informasi mengisolasi perangkat elektronik (*PC, Laptop, Smartphone* dan perangkat lainnya) yang dicurigai mengalami masalah;
c Pemilik informasi tidak melakukan tindakan yang membuat permasalahan tersebut dapat mengancam aset informasi lainnya;
d Pemilik informasi melakukan koordinasi dan melaporkan permasalahan kepada perangkat daerah yang berwenang dan bertanggung jawab memimpin pengelolaan keamanan informasi di pemerintahan Kabupaten Bandung (*Information Security Officer*); dan
e *Information Security Officer* harus membantu penanggulangan permasalahan keamanan informasi berkerjasama dengan pemilik informasi dan pihak terkait lain sesuai dengan aturan yang berlaku.

Bagian Kedua

Mekanisme Layanan Keamanan Informasi Non Elektronik

Pasal 19

Tindakan yang harus dilaksanakan dalam menangani dan merespon insiden yang mengancam Keamanan Informasi non elektronik:

a Pemilik Informasi mengidentifikasi permasalahan dan sumber kebocoran informasi non elektronik.
b Pemilik informasi melakukan koordinasi dan melaporkan permasalahan kepada perangkat daerah yang berwenang dan bertanggung jawab memimpin pengelolaan keamanan informasi di pemerintahan Kabupaten Bandung (Information Security Officer).

c Information Security Officer harus membantu penanggulangan permasalahan keamanan informasi berkerjasama dengan pemilik informasi dan pihak terkait lain sesuai dengan aturan yang berlaku.

BAB XII

MANAJEMEN KEBERLANGSUNGAN KEAMANAN INFORMASI

Pasal 19

Tindakan yang harus diimplementasikan dalam untuk menjamin keberlangsungan keamanan informasi:

a Perangkat daerah yang berwenang dan bertanggung jawab memimpin pengelolaan keamanan informasi di pemerintahan Kabupaten Bandung (*Information Security Officer*) harus membuat rencana keberlangsungan keamanan informasi; dan
b Rencana keberlangsungan Kemanan informasi sebagaimana pada ayat (1) minimal memuat Tugas, Proses, Prosedur dan Kendali untuk menjaga keberlangsungan keamanan informasi.

BAB XIII

KERJASAMA DAN KEMITRAAN

Pasal 20

(1) Pemerintah daerah dapat mengembangkan pola kerjasama dan kemitraan dalam rangka mewujudkan proses keamanan informasi Kabupaten Bandung, sesuai ketentuan peraturan perundang-undangan yang berlaku.
(2) Kerjasama dan kemitraan sebagaimana dimaksud pada ayat (1) dilakukan dengan :
    a. Pemerintah Pusat;
    b. Pemerintah Provinsi;
    c. Pemerintah Kabupaten/Kota;
    d. Perguruan tinggi;
    e. Lembaga penelitian; dan
    f. Pihak lainnya.

BAB XIV

KETENTUAN PENUTUP

Pasal 21

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 28 Desember 2018

BUPATI BANDUNG,

ttd

DADANG M. NASER

Diundangkan di Soreang
Pada tanggal 28 Desember 2018

SEKRETARIS DAERAH
KABUPATEN BANDUNG,

ttd

TEDDY KUSDIANA

BERITA DAERAH KABUPATEN BANDUNG TAHUN 2019 NOMOR 131

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM

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

PENJELASAN
ATAS
PERATURAN BUPATI BANDUNG

NOMOR 131 TAHUN 2018

TENTANG

KEAMANAN INFORMASI DI LINGKUNGAN
PEMERINTAH KABUPATEN BANDUNG

I. UMUM

Kemanan informasi merupakan suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas pemerintahan dan mengurangi resiko yang terjadi yang membahayakan penyelenggaraan pemerintahan.

Untuk mendukung penyelenggaraan keamanan informasi yang terkelola dengan baik agar dapat menjaga seluruh sumber daya informasi secara efisien dan efektif serta terciptanya sinergi di antara Perangkat Daerah di lingkungan pemerintah kabupaten Bandung, perlu ditetapkan peraturan Bupati tentang Penerapan keamanan informasi.

Peraturan Bupati ini dimaksudkan sebagai pedoman umum Penerapan Keamanan Informasi yang berkaitan dengan proses pengamanan data dan informasi dilingkungan Pemerintah Kabupaten Bandung.

Peraturan Bupati ini bertujuan untuk memastikan:

a dilakukannya proses pengamanan informasi guna menjamin ketersediaan data dan informasi yang akurat, mutakhir, terintegrasi, lengkap, akuntabel, dinamis, handal, sahih, mudah diakses dan berkelanjutan;
b diterapkannya Penerapan keamanan informasi secara efektif, efisien, dan konsisten dengan pendekatan berbasis risiko;
c tersusunnya sistem dokumentasi minimum yang diperlukan untuk menerapkan keamanan informasi;
d bahwa *stakeholder* berpartisipasi aktif dalam proses pengamanan informasi;
e terciptanya dukungan terhadap Kerahasiaan (*Confidentiality*), Keaslian (*Authentication*) Keutuhan (*Integrity*), Ketersediaan (*Availibility*) informasi dan Kenirsangkalan (*Nonrepudiation)*;
f data dan informasi yang dihasilkan dan/atau dideseminasikan sesuai dengan kebutuhan *stakeholder* sehingga tercapai efektifitas dan efisiensi pelaksanaan tugas dan layanan pemerintahan.

Ruang lingkup peraturan bupati ini, meliputi Kebijakan Keamanan Informasi, Organisasi Keamanan Informasi, Pengelolaan Aset Informasi, Keamanan Sumber Daya Manusia, Keamanan Fisik & Lingkungan, Manajemen Komunikasi dan Operasi, Pengendalian Akses, Manajemen Kriptografi, Pengembangan, Akuisisi & Pemeliharaan Sistem Informasi, Manajemen Hubungan Pemasok, Manajemen Insiden Keamanan Informasi, Manajemen Keberlangsungan Keamanan Informasi dan Kerjasama dan Kemitraan.

II. PASAL DEMI PASAL.

Pasal 1

Cukup jelas

Pasal 2

Huruf a

Yang dimaksud dengan Kerahasiaan atau *Confidentiality* dalam keamanan informasi adalah Keamanan informasi menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu. Pengertian lain dari *confidentiality* merupakan tindakan pencegahan dari orang atau pihak yang tidak berhak untuk mengakses informasi.

Huruf b

Yang dimaksud dengan Keaslian atau *Authentication* adalah Menjamin dan memastikan identitas pengguna sistem.

Huruf c

Yang dimaksud dengan Keutuhan atau Integrity dalam keamanan informasi adalah Keamanan informasi menjamin kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang mengakibatkan berubah informasi dari aslinya. Pengertian lain dari *integrity* adalah memastikan bahwa informasi tersebut masih utuh, akurat, dan belum dimodifikasi oleh pihak yang tidak berhak.

Huruf d

Yang dimaksud dengan Ketersediaan atau *Availibility* dalam keamanan informasi adalah Keamanan informasi menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tidak bisa digunakan. Pengguna dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses informasi. A*vailability* meyakinkan bahwa pengguna mempunyai kesempatan dan akses pada suatu informasi.

Huruf e

Yang dimaksud dengan Kenirsangkalan *atau Nonrepudiation* adalah Menjamin agar seseorang tidak dapat menyangkal terhadap aktifitas yang telah dilakukan dalam sebuah transaksi sistem informasi atau data.

Pasal 3

Cukup jelas

Pasal 4

Cukup jelas

Pasal 5

Huruf a

Yang dimaksud dengan Pemilik informasi. adalah PD/Bidang/Seksi/Individu ASN yang memiliki aset informasi yang bertanggung jawab atas keamanan aset informasi yang dimiliki dan dikelolanya tersebut.

Huruf b

Yang dimaksud dengan Pengelola informasi adalah PPID Pembantu pada setiap PD dibawah koordinasi PD pengelola TIK Pemerintah Daerah.

Huruf c

Yang dimaksud dengan Pengguna informasi adalah K/L/D/ASN serta Publik yang mempunyai kewenangan untuk menggunakan aset informasi sesuai dengan peraturan perundangan yang berlaku.

Huruf d

Yang dimaksud dengan Information Security Officer adalah ASN yang berwenang dan bertanggung jawab memimpin pengelolaan keamanan informasi di pemerintahan Kabupaten Bandung yang ditetapkan oleh surat keputusan Bupati.

Pasal 6

Cukup jelas

Pasal 7

Cukup jelas

Pasal 8

Cukup jelas

Pasal 9

Cukup jelas

Pasal 10

Cukup jelas

Pasal 11

Cukup jelas

Pasal 12

Cukup jelas

Pasal 13

Cukup jelas

Pasal 14

Cukup jelas

Pasal 15

Cukup jelas

Pasal 16

Cukup jelas

Pasal 17

Cukup jelas

Pasal 18

Cukup jelas

Pasal 19

Cukup jelas

Pasal 20

Cukup jelas

Pasal 21

Cukup jelas

TAMBAHAN BERITA DAERAH KABUPATEN BANDUNG NOMOR 18